Docket No. 250225US2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kenichi TAKEDA, et al. GAU:

SERIAL NO: New Application EXAMINER:

FILED: Herewith

FOR: PRINTER DRIVER PROGRAM AND PRINTER

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-078788	March 20, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

PRCA-03095-US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２０日

出願番号
Application Number: 特願２００３－０７８７８８

[ST. 10/C]: [ＪＰ２００３－０７８７８８]

出願人
Applicant(s): 株式会社リコー

２００３年１１月１０日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０９２７１０

【書類名】　特許願

【整理番号】　0301447

【提出日】　平成15年 3月20日

【あて先】　特許庁長官殿

【国際特許分類】　B41J 29/38

G06F 3/12

【発明の名称】　プリンタドライバプログラムおよびプリンタ装置

【請求項の数】　22

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　武田　健一

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　西脇　浩文

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　澤田　のぞみ

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　大谷　正樹

【特許出願人】

【識別番号】　000006747

【氏名又は名称】　株式会社リコー

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9808514

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　プリンタドライバプログラムおよびプリンタ装置

【特許請求の範囲】

【請求項１】　ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、

所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、

前記暗号化されたアプリ文書データと前記文書認証情報処理手順によって入力された文書認証情報とを含む印刷データを生成する印刷データ生成手順と、

前記印刷データ生成手段によって生成された印刷データをネットワークに接続されたプリンタ装置に送信する送信手順と、

をコンピュータに実行させるプリンタドライバプログラム。

【請求項２】　ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、

前記プリンタ装置との間で予め定められた第１の鍵情報を前記プリンタ装置から取得して、第１の鍵情報に基づいて第２の鍵情報を生成する鍵生成手順と、

所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、

前記文書認証情報処理手段によって入力された前記文書認証情報と前記暗号化されたアプリ文書データとを含む印刷データを生成する印刷データ生成手順と、

前記鍵生成手段によって生成された第２の鍵情報によって前記印刷データを暗号化する暗号化手順と、

前記暗号化手段によって暗号化された印刷データと前記第２の鍵情報を、ネットワークに接続されたプリンタ装置に送信する送信手順と、

をコンピュータに実行させるプリンタドライバプログラム。

【請求項３】　前記第１の鍵情報を前記プリンタ装置に要求する要求手順をさらにコンピュータに実行させる請求項２に記載のプリンタドライバプログラム。

【請求項４】　ネットワークに接続された時点で、接続通知を前記プリンタ

装置に送信し、前記接続通知の送信後に、前記プリンタ装置から前記第１の鍵情報を受信する受信手順をさらにコンピュータに実行させる請求項２に記載のプリンタドライバプログラム。

【請求項５】　ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、

所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、

前記文書認証情報処理手順によって入力された前記文書認証情報と前記暗号化されたアプリ文書データとを含む印刷データを生成する印刷データ生成手順と、

プリンタ装置から取得した公開鍵情報によって前記印刷データを暗号化する暗号化手順と、

前記暗号化手順によって暗号化された印刷データとクライアント装置に固有の識別情報を、ネットワークに接続されたプリンタ装置に送信する送信手順と、

をコンピュータに実行させるプリンタドライバプログラム。

【請求項６】　前記公開鍵情報を前記プリンタ装置に要求する要求手順をさらにコンピュータに実行させる請求項５に記載のプリンタドライバプログラム。

【請求項７】　ネットワークに接続された時点で、接続通知を前記プリンタ装置に送信し、前記接続通知を送信後に、前記プリンタ装置から前記公開鍵情報を受信する受信手順をさらにコンピュータに実行させる請求項５に記載のプリンタドライバプログラム。

【請求項８】　印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させるジョブ認証情報処理手順をさらにコンピュータに実行させ、

前記印刷データ生成手順は、さらに前記ジョブ認証情報処理手順によって入力された前記ジョブ認証情報を含む前記印刷データを生成することを特徴とする請求項２～７のいずれか一つに記載のプリンタドライバプログラム。

【請求項９】　前記文書認証情報処理手段によって入力された文書認証情報から印刷ジョブを開始させるためのジョブ認証情報を生成するジョブ認証情報処理手順をさらにコンピュータに実行させ、

前記印刷データ生成手順は、さらに前記ジョブ認証情報処理手順によって生成

された前記ジョブ認証情報を含む前記印刷データを生成することを特徴とする請求項２～７のいずれか一つに記載のプリンタドライバプログラム。

【請求項１０】　前記ジョブ認証情報処理手順は、前記文書認証情報処理手段によって入力された文書認証情報と同一データを前記ジョブ認証情報として生成することを特徴とする請求項９に記載のプリンタドライバプログラム。

【請求項１１】　ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、

前記クライアント装置から受信した印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、

前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、

を備えたことを特徴とするプリンタ装置。

【請求項１２】　ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、

前記クライアント装置との間で予め定められた第１の鍵情報を生成し、生成された前記第１の鍵情報を前記クライアント装置に送信する第１の鍵情報生成手段と、

前記クライアント装置から受信した前記第１の鍵情報に関連する第２の鍵情報から前記第１の鍵情報を生成するとともに、前記クライアント装置から受信した印刷データを、前記第１の鍵情報によって復号化する復号化手段と、

前記印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、

前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、

を備えたことを特徴とするプリンタ装置。

【請求項１３】　前記第１の鍵生成手段は、前記クライアント装置から前記第１の鍵情報の要求を受信した場合に、前記第１の鍵情報を生成し、生成された前記第１の鍵情報を、直ちに要求のあった前記クライアント装置に送信することを特徴とする請求項１２に記載のプリンタ装置。

【請求項１４】　前記第１の鍵生成手段は、前記クライアント装置から前記第１の鍵情報の要求を受信した場合に、前記第１の鍵情報を生成し、生成された前記第１の鍵情報を、印刷可能な状態となった時点で要求のあった前記クライアント装置に送信することを特徴とする請求項１２に記載のプリンタ装置。

【請求項１５】　前記第１の鍵生成手段は、前記第１の鍵情報を生成し、前記クライアント装置がネットワークに接続された時点で前記クライアント装置に送信することを特徴とする請求項１２に記載のプリンタ装置。

【請求項１６】　前記復号化手段は、前記クライアント装置から前記第２の鍵情報を受信した場合に、前記第１の鍵情報生成手段によって生成された前記第１の鍵情報と、受信した第２の鍵情報から生成された第１の鍵情報とを比較し、両第１の鍵情報が一致する場合にのみ前記印刷データの復号化を行うことを特徴とする請求項１２～１５のいずれか一つに記載のプリンタ装置。

【請求項１７】　ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、

クライアント装置に固有の識別情報に対する秘密鍵情報から公開鍵情報を生成し、クライアント装置に送信する公開鍵処理手段と、

前記クライアント装置から受信した印刷データを、前記クライアント装置から受信した識別情報に対応する秘密鍵情報によって復号化する復号化手段と、

前記印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、

前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、

を備えたことを特徴とするプリンタ装置。

【請求項１８】　前記クライアント装置から前記公開鍵情報の要求を受信した場合に、前記秘密鍵情報を生成する秘密鍵生成手段と、

前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を直ちに前記クライアント装置に送信する公開鍵処理手段と、

をさらに備えたことを特徴とする請求項１７に記載のプリンタ装置。

【請求項１９】　前記クライアント装置から前記公開鍵情報の要求を受信した場合に、前記秘密鍵情報を生成する秘密鍵生成手段と、

前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を、印刷可能な状態になった時点で前記クライアント装置に送信する公開鍵処理手段と、

をさらに備えたことを特徴とする請求項１７に記載のプリンタ装置。

【請求項２０】　前記クライアント装置に対する前記秘密鍵情報を生成する秘密鍵生成手段と、

前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を、前記クライアント装置がネットワークに接続された時点で前記クライアント装置に送信する公開鍵処理手段と、

をさらに備えたことを特徴とする請求項１７に記載のプリンタ装置。

【請求項２１】　前記クライアント装置の識別情報と前記秘密鍵情報と前記秘密鍵情報の有効期間とを対応付けた鍵管理情報を記憶する記憶手段をさらに備え、

前記復号化手段は、前記クライアント装置から前記クライアント情報を受信した場合に、前記鍵管理情報を参照して、前記クライアント情報に対応する前記秘密鍵情報が前記有効期限の範囲内にあるか否かを判断し、前記有効期限の範囲内にある場合にのみ前記印刷データを復号化することを特徴とする請求項１７～２０のいずれか一つに記載のプリンタ装置。

【請求項２２】　前記復号化手段は、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させ、前記印刷データを復号化することを特徴とする請求項１２～２０のいずれか一つに記載のプリンタ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、暗号化されたアプリケーションの文書をプリンタ装置に印刷要求を行うプリンタドライバプログラム、暗号化されたアプリケーションの文書を印刷するプリンタ装置に関する。

【０００２】

【従来の技術】

たとえば、Ａｄｏｂｅ（Ｒ）社のＡｃｒｏｂａｔ　Ｒｅａｄｅｒ（Ｒ）のようなアプリケーションでは、文書内容を他人に閲覧できないようにするために、文書パスワードのような文書認証情報を入力して文書データを暗号化して保存する機能を備えている（非特許文献１参照）。

【０００３】

クライアント装置であるＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）でこのような暗号化された文書データを作成して、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などのネットワークに接続されたプリンタ装置で印刷する場合には、アプリケーション上で文書パスワードを入力して暗号化された文書を復号化してから、復号化された文書をプリンタドライバに渡し、プリンタドライバから復号化された文書ファイルをネットワーク上のプリンタ装置に送信してプリンタ装置でそのまま印刷している。

【０００４】

また、このような暗号化された文書を他人が勝手に印刷することを回避するために、アプリケーションで文書を復号化して印刷要求を行う際に、プリンタドライバ側で印刷ジョブ毎のジョブパスワードをユーザに入力させる。そして、文書データを入力されたジョブパスワードとともにプリンタ装置に送信する。図１７は、このような従来のプリンタドライバとプリンタ装置間を流れる印刷データの構造を示すデータ構造図である。図１７に示すように、ＰＪＬジョブパスワード指定が印刷データであるＰＤＦ文書データ（平文）の先頭に付加されたデータ構造となっている。

【０００５】

そして、プリンタ装置側ではユーザに認証パスワードを入力させて、正当な認証パスワードである場合にのみ印刷ジョブを開始して、文書を印刷するようになっている。

【０００６】

【非特許文献１】

Ａｄｏｂｅ（Ｒ）社ホームページ「Ａｄｏｂｅ　Ａｃｒｏｂａｔなら
ＰＤＦがもっと使える」（ｈｔｔｐ：／／ｗｗｗ．ａｄｏｂｅ．ｃｏ．ｊｐ／ａ
ｃｒｏｆａｍｉｌｙ／ｆｅａｔｕｒｅｓ／ａｃｒｏ＿ｎｉｋｋｅｉ／ｐａｇｅ４
．ｈｔｍｌ）

【０００７】

【発明が解決しようとする課題】

しかしながら、このような従来のプリンタドライバやプリンタ装置では、アプリケーション上で暗号化された文書であっても、印刷する段階で復号化しなければならないため、ＰＣからプリンタ装置までのネットワーク上を平文の文書データが流れてしまい、悪意のある第三者によって平文の文書データが傍受されてしまうおそれがある。

【０００８】

また、印刷ジョブ毎のジョブパスワードによって悪意のある第三者による暗号化文書の印刷を防止してる場合であっても、ジョブパスワードが平文のために、ネットワーク上で第三者に傍受されてしまう可能性がある。また、プリンタ装置のハードディスク装置（ＨＤＤ）やメモリなどの記憶媒体には復号化された文書データが一時的に保存されるため、プリンタ装置のシステム管理者が保存された平文の文書データを参照することができてしまう。

【０００９】

このように、従来のプリンタドライバやプリンタ装置では、アプリケーションで暗号化された文書データを印刷する場合に、セキュリティが低下してしまうという問題があった。

【００１０】

この発明は上記に鑑みてなされたもので、アプリケーションで暗号化された文書データを印刷する場合においてもセキュリティを向上させることができるプリンタドライバプログラムおよびプリンタ装置を得ることを目的とする。

【００１１】

【課題を解決するための手段】

上記目的を達成するため、請求項１にかかる発明は、ネットワークに接続され

たプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、前記暗号化されたアプリ文書データと前記文書認証情報処理手順によって入力された文書認証情報とを含む印刷データを生成する印刷データ生成手順と、前記印刷データ生成手段によって生成された印刷データをネットワークに接続されたプリンタ装置に送信する送信手順と、をコンピュータに実行させるプリンタドライバプログラムである。

【００１２】

この請求項１の発明によれば、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させ、暗号化されたアプリ文書データと入力された文書認証情報とを含む印刷データを生成してネットワークに接続されたプリンタ装置に送信することで、暗号化されたアプリ文書データを復号化せずにプリンタ装置に送信して、同時に送信する文書認証情報によってプリンタ装置側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができる。また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【００１３】

また、請求項２にかかる発明は、ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、前記プリンタ装置との間で予め定められた第１の鍵情報を前記プリンタ装置から取得して、第１の鍵情報に基づいて第２の鍵情報を生成する鍵生成手順と、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、前記文書認証情報処理手段によって入力された前記文書認証情報と前記暗号化されたアプリ文書データとを含む印刷データを生成する印刷データ生成手順と、前記鍵生成手段に

よって生成された第２の鍵情報によって前記印刷データを暗号化する暗号化手順と、前記暗号化手段によって暗号化された印刷データと前記第２の鍵情報を、ネットワークに接続されたプリンタ装置に送信する送信手順と、をコンピュータに実行させるプリンタドライバプログラムである。

【００１４】

この請求項２の発明によれば、プリンタ装置から取得した第１の鍵情報から第２の鍵情報を生成し、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させ、入力された文書認証情報と暗号化されたアプリ文書データとを含む印刷データを生成し、生成された第２の鍵情報によって印刷データを暗号化し、暗号化された印刷データと第２の鍵情報をネットワークに接続されたプリンタ装置に送信することで、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を第２の鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【００１５】

また、請求項３にかかる発明は、請求項２に記載のプリンタドライバプログラムにおいて、前記第１の鍵情報を前記プリンタ装置に要求する要求手順をさらにコンピュータに実行させるものである。

【００１６】

この請求項３の発明によれば、第１の鍵情報を前記プリンタ装置に要求することで、印刷ジョブごとに異なる第１の鍵情報を取得することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【００１７】

また、請求項４にかかる発明は、請求項２に記載のプリンタドライバプログラ

ムにおいて、ネットワークに接続された時点で、接続通知を前記プリンタ装置に送信し、前記接続通知の送信後に、前記プリンタ装置から前記第１の鍵情報を受信する受信手順をさらにコンピュータに実行させるものである。

【００１８】

この請求項４の発明によれば、ネットワークに接続された時点で、接続通知をプリンタ装置に送信して、かかる接続通知の送信後にプリンタ装置から第１の鍵情報を受信することで、印刷する度に第１の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができる。

【００１９】

また、請求項５にかかる発明は、ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラムであって、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させる文書認証情報処理手順と、前記文書認証情報処理手順によって入力された前記文書認証情報と前記暗号化されたアプリ文書データとを含む印刷データを生成する印刷データ生成手順と、プリンタ装置から取得した公開鍵情報によって前記印刷データを暗号化する暗号化手順と、前記暗号化手順によって暗号化された印刷データとクライアント装置に固有の識別情報を、ネットワークに接続されたプリンタ装置に送信する送信手順と、をコンピュータに実行させるプリンタドライバプログラムである。

【００２０】

この請求項５の発明によれば、所定のアプリケーションによって暗号化されたアプリ文書データを復号化するための文書認証情報をユーザに入力させ、入力された文書認証情報と暗号化されたアプリ文書データとを含む印刷データを生成し、プリンタ装置から取得した公開鍵情報によって印刷データを暗号化し、暗号化された印刷データとクライアント装置に固有の識別情報を、ネットワークに接続されたプリンタ装置に送信することで、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を公開鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある

第三者が傍受することを確実に防止することができる。また、プリンタ装置で秘密鍵情報を用いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【００２１】

また、請求項６にかかる発明は、請求項５に記載のプリンタドライバプログラムにおいて、前記公開鍵情報を前記プリンタ装置に要求する要求手順をさらにコンピュータに実行させるものである。

【００２２】

この請求項６の発明によれば、公開鍵情報をプリンタ装置に要求することで、印刷ジョブごとに異なる公開鍵情報を取得することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【００２３】

また、請求項７にかかる発明は、請求項５に記載のプリンタドライバプログラムにおいて、ネットワークに接続された時点で、接続通知を前記プリンタ装置に送信し、前記接続通知を送信後に、前記プリンタ装置から前記公開鍵情報を受信する受信手順をさらにコンピュータに実行させるものである。

【００２４】

この請求項７の発明によれば、ネットワークに接続された時点で、接続通知をプリンタ装置に送信し、かかる接続通知を送信後にプリンタ装置から公開鍵情報を受信することで、印刷する度に第１の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができる。

【００２５】

また、請求項８にかかる発明は、請求項２～７のいずれか一つに記載のプリンタドライバプログラムにおいて、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させるジョブ認証情報処理手順をさらにコンピュータに実行させ、前記印刷データ生成手順は、さらに前記ジョブ認証情報処理手順によって入力

された前記ジョブ認証情報を含む前記印刷データを生成することを特徴とする。

【００２６】

この請求項８の発明によれば、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させ、入力されたジョブ認証情報を含む印刷データを生成することで、暗号化されたアプリ文書データの印刷時において、アプリ文書データを暗号化された状態のまま、さらに印刷ジョブ毎に認証を行うことができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【００２７】

また、請求項９にかかる発明は、請求項２～７のいずれか一つに記載のプリンタドライバプログラムにおいて、前記文書認証情報処理手段によって入力された文書認証情報から印刷ジョブを開始させるためのジョブ認証情報を生成するジョブ認証情報処理手順をさらにコンピュータに実行させ、前記印刷データ生成手順は、さらに前記ジョブ認証情報処理手順によって生成された前記ジョブ認証情報を含む前記印刷データを生成することを特徴とするものである。

【００２８】

この請求項９の発明によれば、入力された文書認証情報から印刷ジョブを開始させるためのジョブ認証情報を生成し、ジョブ認証情報を含む印刷データを生成することで、印刷ジョブ毎に認証に必要なジョブ認証情報を、アプリ文書データの暗号化に必要な文書認証情報から自動的に生成することができるので、ユーザに何度も認証情報を入力させる手間が省け、ユーザの便宜となる。

【００２９】

また、請求項１０にかかる発明は、請求項９に記載のプリンタドライバプログラムにおいて、前記ジョブ認証情報処理手順は、前記文書認証情報処理手段によって入力された文書認証情報と同一データを前記ジョブ認証情報として生成することを特徴とする。

【００３０】

この請求項１０の発明によれば、入力された文書認証情報と同一データを前記

ジョブ認証情報として生成することで、文書認証情報からジョブ認証情報を簡易に生成することができ、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させつつ迅速に行うことができる。

【００３１】

また、請求項１１にかかる発明は、ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、前記クライアント装置から受信した印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、を備えたことを特徴とする。

【００３２】

この請求項１１の発明によれば、クライアント装置から受信した印刷データに含まれる文書認証情報によって暗号化されたアプリ文書データを復号化し、復号化されたアプリ文書データを印刷することで、アプリ文書データを暗号化されたままクライント装置から受信して、同時に送信する文書認証情報によってプリンタ装置側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができる。また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【００３３】

また、請求項１２にかかる発明は、ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、前記クライアント装置との間で予め定められた第１の鍵情報を生成し、生成された前記第１の鍵情報を前記クライアント装置に送信する第１の鍵情報生成手段と、前記クライアント装置から受信した前記第１の鍵情報に関連する第２の鍵情報から前記第１の鍵情報を生成するとともに、前記クライアント装置から受信した印刷データを、前記第１の鍵情報によって復号化する復号化手段と、前記印刷データに含ま

れる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、を備えたことを特徴とする。

【００３４】

この請求項１２の発明によれば、クライアント装置との間で予め定められた第１の鍵情報を生成し、生成された第１の鍵情報をクライアント装置に送信し、クライアント装置から受信した第２の鍵情報から第１の鍵情報を生成するとともに、クライアント装置から受信した印刷データを、第１の鍵情報によって復号化し、印刷データに含まれる文書認証情報によって暗号化されたアプリ文書データを復号化し、復号化されたアプリ文書データを印刷することで、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を第２の鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【００３５】

また、請求項１３にかかる発明は、請求項１２に記載のプリンタ装置において、前記第１の鍵生成手段は、前記クライアント装置から前記第１の鍵情報の要求を受信した場合に、前記第１の鍵情報を生成し、生成された前記第１の鍵情報を、直ちに要求のあった前記クライアント装置に送信することを特徴とする。

【００３６】

この請求項１３の発明によれば、クライアント装置から前記第１の鍵情報の要求を受信した場合に、前記第１の鍵情報を生成し、生成された前記第１の鍵情報を、直ちに要求のあった前記クライアント装置に送信することで、要求された時点で直ちに印刷ジョブごとに異なる第１の鍵情報を送信することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【００３７】

また、請求項１４にかかる発明は、請求項１２に記載のプリンタ装置において、前記第１の鍵生成手段は、前記クライアント装置から前記第１の鍵情報の要求を受信した場合に、前記第１の鍵情報を生成し、生成された前記第１の鍵情報を、印刷可能な状態となった時点で要求のあった前記クライアント装置に送信することを特徴とする。

【００３８】

この請求項１４の発明によれば、クライアント装置から第１の鍵情報の要求を受信した場合に、第１の鍵情報を生成し、生成された第１の鍵情報を、印刷可能な状態となった時点で要求のあった前記イアント装置に送信することで、要求があった時点から印刷開始時までに時間差がある場合に、実際に印刷開始時に第１の鍵情報を送信することができるので、要求時点から印刷開始時点までの間に第三者が傍受することを回避することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【００３９】

また、請求項１５にかかる発明は、請求項１２に記載のプリンタ装置において、前記第１の鍵生成手段は、前記第１の鍵情報を生成し、前記クライアント装置がネットワークに接続された時点で前記クライアント装置に送信することを特徴とする。

【００４０】

この請求項１５の発明によれば、第１の鍵情報を生成し、クライアント装置がネットワークに接続された時点でクライアント装置に送信することで、クライアント装置側で印刷する度に第１の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができる。

【００４１】

また、請求項１６にかかる発明は、請求項１２～１５のいずれか一つに記載のプリンタ装置において、前記復号化手段は、前記クライアント装置から前記第２の鍵情報を受信した場合に、前記第１の鍵情報生成手段によって生成された前記第１の鍵情報と、受信した第２の鍵情報から生成された第１の鍵情報とを比較し

、両第１の鍵情報が一致する場合にのみ前記印刷データの復号化を行うことを特徴とする。

【００４２】

この請求項１６の発明によれば、クライアント装置から第２の鍵情報を受信した場合に、生成された第１の鍵情報と、受信した第２の鍵情報から生成された第１の鍵情報とを比較し、両第１の鍵情報が一致する場合にのみ印刷データの復号化を行うことで、第１の鍵情報の改ざんされた場合に暗号化されたアプリ文書データの印刷を未然に防止することができ、セキュリティの向上を図ることができる。

【００４３】

また、請求項１７にかかる発明は、ネットワークに接続されたクライアント装置からの印刷要求を受信して印刷処理を行うプリンタ装置であって、クライアント装置に固有の識別情報に対する秘密鍵情報から公開鍵情報を生成し、クライアント装置に送信する公開鍵処理手段と、前記クライアント装置から受信した印刷データを、前記クライアント装置から受信した識別情報に対応する秘密鍵情報によって復号化する復号化手段と、前記印刷データに含まれる前記文書認証情報によって前記暗号化されたアプリ文書データを復号化する文書復号化手段と、前記文書復号化手段によって復号化されたアプリ文書データを印刷する印刷手段と、を備えたことを特徴とする。

【００４４】

この請求項１７の発明によれば、クライアント装置に固有の識別情報に対する秘密鍵情報から公開鍵情報を生成し、クライアント装置に送信し、クライアント装置から受信した印刷データをクライアント装置から受信した識別情報に対応する秘密鍵情報によって復号化し、印刷データに含まれる文書認証情報によって暗号化されたアプリ文書データを復号化し、復号化されたアプリ文書データを印刷することで、アプリ文書データを暗号化された状態のまま、しかも復号化するための文書認証情報を公開鍵情報で暗号化された状態でクライアント装置から受信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置で秘密鍵情報を用

いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【００４５】

また、請求項１８にかかる発明は、請求項１７に記載のプリンタ装置において、前記クライアント装置から前記公開鍵情報の要求を受信した場合に、前記秘密鍵情報を生成する秘密鍵生成手段と、前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を直ちに前記クライアント装置に送信する公開鍵処理手段と、をさらに備えたことを特徴とする。

【００４６】

この請求項１８の発明によれば、クライアント装置から公開鍵情報の要求を受信した場合に、秘密鍵情報を生成し、生成された秘密鍵情報から公開鍵情報を生成し、生成された公開鍵情報を直ちにクライアント装置に送信することで、要求された時点で直ちに印刷ジョブごとに異なる公開鍵情報を送信することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【００４７】

また、請求項１９にかかる発明は、請求項１７に記載のプリンタ装置において、前記クライアント装置から前記公開鍵情報の要求を受信した場合に、前記秘密鍵情報を生成する秘密鍵生成手段と、前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を、印刷可能な状態になった時点で前記クライアント装置に送信する公開鍵処理手段と、をさらに備えたことを特徴とする。

【００４８】

この請求項１９の発明によれば、クライアント装置から公開鍵情報の要求を受信した場合に秘密鍵情報を生成し、生成された秘密鍵情報から公開鍵情報を生成し、生成された前記公開鍵情報を、印刷可能な状態になった時点で前記イアント装置に送信することで、要求があった時点から印刷開始時までに時間差がある場

合に、実際に印刷開始時に公開鍵情報を送信することができるので、要求時点から印刷開始時点までの間に第三者が傍受することを回避することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【００４９】

また、請求項２０にかかる発明は、請求項１７に記載のプリンタ装置において、前記クライアント装置に対する前記秘密鍵情報を生成する秘密鍵生成手段と、前記秘密鍵生成手段によって生成された秘密鍵情報から前記公開鍵情報を生成し、生成された前記公開鍵情報を、前記クライアント装置がネットワークに接続された時点で前記クライアント装置に送信する公開鍵処理手段と、をさらに備えたことを特徴とする。

【００５０】

この請求項２０の発明によれば、クライアント装置に対する秘密鍵情報を生成し、生成された秘密鍵情報から公開鍵情報を生成し、生成された公開鍵情報を、クライアント装置がネットワークに接続された時点でクライアント装置に送信することで、クライアント装置側で印刷する度に公開鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができる。

【００５１】

また、請求項２１にかかる発明は、請求項１７～２０のいずれか一つに記載のプリンタ装置において、前記クライアント装置の識別情報と前記秘密鍵情報と前記秘密鍵情報の有効期間とを対応付けた鍵管理情報を記憶する記憶手段をさらに備え、前記復号化手段は、前記クライアント装置から前記クライアント情報を受信した場合に、前記鍵管理情報を参照して、前記クライアント情報に対応する前記秘密鍵情報が前記有効期限の範囲内にあるか否かを判断し、前記有効期限の範囲内にある場合にのみ前記印刷データを復号化することを特徴とする。

【００５２】

この請求項２１の発明によれば、クライアント装置の識別情報と秘密鍵情報と秘密鍵情報の有効期間とを対応付けた鍵管理情報を記憶し、クライアント装置からクライアント情報を受信した場合に、鍵管理情報を参照してクライアント情報

に対応する秘密鍵情報が前記有効期限の範囲内にあるか否かを判断し、有効期限の範囲内にある場合にのみ印刷データを復号化することで、有効期限切れで第三の傍受されたおそれのある秘密鍵情報によるアプリ文書データの復号化および印刷を防止することができ、セキュリティをより向上させることができる。

【００５３】

また、請求項２２にかかる発明は、請求項１２～２０のいずれか一つに記載のプリンタ装置において、前記復号化手段は、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させ、前記印刷データを復号化することを特徴とする。

【００５４】

この請求項２２の発明によれば、印刷ジョブを開始させるためのジョブ認証情報をユーザに入力させ、前記印刷データを復号化することで、暗号化されたアプリ文書データの印刷時において、アプリ文書データを暗号化された状態のまま、さらに印刷ジョブ毎に認証を行うことができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【００５５】

【発明の実施の形態】

以下に添付図面を参照して、この発明にかかるプリンタドライバプログラムおよびプリンタ装置の好適な実施の形態を詳細に説明する。

【００５６】

（実施の形態１）

図１は、この発明の実施の形態１であるクライアント装置（ＰＣ）１００およびプリンタ装置１３０の機能的構成を示すブロック図である。この実施の形態１にかかるＰＣ１００では、ＰＣ上のアプリケーション１２０であるＡｃｒｏｂａｔ（Ｒ）によってＰＤＦ文書データを作成して暗号化し、文書パスワードの入力で復号化できる暗号化ＰＤＦ文書データをそのまま（復号化せず）、プリンタ装置１３０に送信し、プリンタ装置１３０で印刷するようになっている。

【００５７】

プリンタ装置１３０とＰＣ１００とは、ＬＡＮ１５１等のネットワークによって接続されている。ＰＣ１００は、図１に示すように、プリンタドライバ１１０がインストールされており、このプリンタドライバ１１０は、ＰＤＬ処理部１１１と、文書パスワード処理部１１２と、ユーザインタフェース部１１３と、ホストＩ／Ｆ制御部１１４とを主に備えている。

【００５８】

文書パスワード処理部１１２は、アプリケーション１２０内部で暗号化されたＰＤＦ文書データを復号化するために必要な文書パスワードの入力指示を要求し、入力された文書パスワードを受け付ける。そして、ユーザから入力された文書パスワードをＰＪＬ文書パスワード指定データとして暗号化ＰＤＦ文書データの先頭に付加する。そして、ＰＪＬ文書パスワード指定データが付加された暗号化ＰＤＦ文書データの後尾に印刷ジョブに関するデータであるＰＪＬデータを付加する。そして、これらのＰＪＬ文書パスワード指定データとＰＪＬデータとが付加された暗号化ＰＤＦ文書データとを印刷データとする。この文書パスワードは、本発明における文書認証情報を構成する。

【００５９】

ＰＤＬ処理部１１１は、ＰＤＦ文書データ（暗号化されていないデータ）の印刷の際に使用されるものであり、暗号化されていないＰＤＦ文書データの印刷文書データをＰＤＬデータ（ＰＤＬ：Ｐａｇｅ　Ｄｅｓｃｒｉｐｔｏｎ　Ｌａｎｇｕａｇｅ：ページ記述言語）に変換して印刷データを生成するものである。

【００６０】

ユーザインタフェース部１１３は、モニタ１１５に各種画面を表示するとともに、ユーザによるキーボード１１６からの入力イベントを受け付けるものである。

【００６１】

ホストＩ／Ｆ制御部１１４は、暗号化されたＰＤＦ文書データをホストＩ／Ｆ１１７からＬＡＮ１５１を介してプリンタ装置１３０に送信するものである。

【００６２】

プリンタ装置１３０には、プリンタコントローラ１４０が装着されており、こ

のプリンタコントローラ１４０は、ＰＤＬ処理部１４２と、ＰＪＬ処理部１４１と、ホストＩ／Ｆ制御部１４３と、パネル制御部１４４と、蓄積制御部１４５と、印刷制御部１４６とを主に備えている。

【００６３】

ＰＪＬ処理部１４１は、ＰＣ１００から受信した印刷データの先頭に付加されたプリンタジョブ言語（ＰＪＬ：Ｐｒｉｎｔｅｒ　Ｊｏｂ　Ｌａｎｇｕａｇｅ）で記述されたＰＪＬ文書パスワード指定を解釈して、文書パスワードを取得するものである。ＰＪＬ処理部１４１は、この他刷ジョブに関する各種制御を行う。

【００６４】

ＰＤＬ処理部１４２は、ＰＪＬ処理部１４１によって取得された文書パスワードの正当性を判断し、正当である場合には、この文書パスワードを用いて暗号化されたＰＤＦ文書データを復号化し、描画データを生成する。このＰＤＬ処理部１４２は、本発明における文書復号化手段を構成する。

【００６５】

ホストＩ／Ｆ制御部１４３は、ＬＡＮ１１５、ホストＩ／Ｆ１４７を介してＰＣ１００から印刷データを受信するものである。

【００６６】

パネル制御部１４４は、操作パネル１４８に対する表示出力、入力イベントの取得などを制御するものである。蓄積制御部１４５は、ハードディスク装置（ＨＤＤ）１４９やメモリに対するリード／ライトを制御するものである。印刷制御部１４６は、印刷エンジン１５０に対する印刷要求を制御するものである。

【００６７】

次に、以上のように構成された本実施の形態のプリンタドライバおよびプリンタ装置１３０による暗号化ＰＤＦ文書データの印刷処理について説明する。図２は、本実施の形態のプリンタドライバおよびプリンタ装置１３０による暗号化ＰＤＦ文書データの印刷処理の手順を示すフローチャートである。

【００６８】

まず、ユーザがアプリケーション１２０（Ａｃｒｏｂａｔ（Ｒ）またはＡｃｒｏｂａｔ　Ｒｅａｄｅｒ（Ｒ））でＰＤＦ文書を文書パスワードによって暗号化

し、暗号化した状態のままアプリケーション１２０の印刷画面でプリンタ装置１３０のＩＰアドレスを指定して印刷コマンドを発行した場合を考える。

【００６９】

このとき、プリンタドライバ１１０では、文書パスワード処理部１１２が文書パスワード入力画面の表示要求をユーザインタフェース部１１３に対して行うことにより、ユーザインタフェース部１１３は文書パスワード入力画面をモニタ１１５に表示する（ステップＳ２０１）。

【００７０】

ユーザが文書パスワード入力画面から暗号化ＰＤＦ文書データに対する文書パスワードをキーボード１１６から入力すると、そのキーイベントをユーザインタフェース部１１３が取得する。そして、文書パスワード処理部１１２は、取得した文書パスワードをＰＪＬ文書パスワード指定データとして暗号化ＰＤＦ文書データの先頭に付加する（ステップＳ２０２）。そして、文書パスワード処理部１１２によって、ＰＪＬ文書パスワード指定データが付加された暗号化ＰＤＦ文書データの後尾にＰＪＬデータを付加し、これらのデータを印刷データとして生成する（ステップＳ２０３）。生成された印刷データは、ホストＩ／Ｆ制御部１１４によって、プリンタ装置１３０に送信される（ステップＳ２０４）。

【００７１】

図４は、本実施の形態のプリンタドライバ１１０で生成される印刷データの構造を示すデータ構造図である。図２に示すように、印刷データは、ＰＪＬ文書パスワード指定（平文）と暗号化ＰＤＦ文書データとＰＪＬデータとから構成される。なお、ＰＪＬデータは付加されていない場合もある。

【００７２】

プリンタ装置１３０では、ホストＩ／Ｆ制御部１４３で印刷データを受信して（ステップＳ２０５）、受信した印刷データのデータ解釈処理を行い（ステップＳ２０６）、印刷制御部１４６によって印刷実行を行う（ステップＳ２０７）。

【００７３】

ここで、印刷データの解釈処理について説明する。図３は、印刷データの解釈処理の手順を示すフローチャートである。まず、ＰＪＬ処理部１４１によって、

印刷データに含まれるＰＪＬ文書パスワード指定を解釈し、文書パスワードを取得する（ステップＳ３０１）。そして、ＰＤＬ処理部１４２によって、取得した文書パスワードと暗号化ＰＤＦ文書データに含まれる文書パスワードとが一致するか否かをチェックすることにより、印刷データに含まれた文書パスワードの正当性を判断する（ステップＳ３０２）。ここで、暗号化ＰＤＦ文書データに含まれる文書パスワードの取得は、アプリケーション１２０に提供されるパスワード取得関数を呼び出すことにより行う。

【００７４】

そして、両文書パスワードが一致する場合には、文書パスワードが正当であると判断し、ＰＤＬ処理部１４２によって暗号化ＰＤＦ文書データを復号化して、描画データを生成する（ステップＳ３０３）。一方、両文書パスワードが一致しない場合には、文書パスワードが不当であると判断し、印刷データを破棄して印刷処理の実行は行わない（ステップＳ３０４）。

【００７５】

このように実施の形態１のプリンタドライバ１１０およびプリンタ装置１３０では、アプリケーション１２０によって暗号化されたアプリ文書データを復号化するための文書パスワードと、暗号化されたＰＤＦ文書データを含む印刷データをネットワークに接続されたプリンタ装置１３０に送信しているので、暗号化されたＰＤＦ文書データを復号化せずにプリンタ装置１３０に送信して、同時に送信する文書パスワードによってプリンタ装置１３０側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができる。また、プリンタ装置１３０で復号化するまでＨＤＤ１４９などにＰＤＦ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってＰＤＦ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【００７６】

（実施の形態２）

図５は、実施の形態２のクライアント装置（ＰＣ）５００およびプリンタ装置

５３０の機能的構成を示すブロック図である。この実施の形態２にかかるＰＣ５００では、ＰＣ上のアプリケーション１２０であるＡｃｒｏｂａｔ（Ｒ）によってＰＤＦ文書データを作成して暗号化し、文書パスワードと文書パスワードの入力で復号化できる暗号化ＰＤＦ文書データを、ＰＣ５００とプリンタ装置５３０との間で定められたＳＥＥＤによって暗号化して、プリンタ装置１３０に送信し、プリンタ装置５３０でＳＥＥＤ元によって復号化して印刷するようになっている。

【００７７】

プリンタ装置５３０とＰＣ５００とは、ＬＡＮ１５１等のネットワークによって接続されている。ＰＣ５００は、図５に示すように、プリンタドライバ５１０がインストールされており、このプリンタドライバ１１０は、ＰＤＬ処理部１１１と、文書パスワード処理部１１２と、ＳＥＥＤ生成部５１１と、暗号化部５１２と、ジョブ制御部５１３と、ユーザインタフェース部１１３と、ホストＩ／Ｆ制御部１１４とを主に備えている。

【００７８】

文書パスワード処理部１１２は、アプリケーション１２０内部で暗号化されたＰＤＦ文書データを復号化するために必要な文書パスワードの入力指示を要求し、入力された文書パスワードを受け付ける。そして、ユーザから入力された文書パスワードをＰＪＬ文書パスワード指定データとして暗号化ＰＤＦ文書データの先頭に付加する。その他の機能は実施の形態１と文書パスワード処理部と同様である。

【００７９】

ジョブ制御部５１３は、プリンタ装置５３０に対して、ＳＥＥＤ元の要求を行うものであり、ＳＥＥＤ生成部５１１は、プリンタ装置５３０から受信したＳＥＥＤ元からＳＥＥＤを生成するものである。

【００８０】

暗号化部５１２は、生成されたＳＥＥＤによって、ＰＪＬ文書パスワード指定データ、暗号化ＰＤＦ文書データ、および印刷ジョブに関するデータであるＰＪＬデータを暗号化するものである。なお、ＰＤＬ処理部１１１は、実施の形態１

と同様の機能を有する。

【００８１】

ユーザインタフェース部１１３は、実施の形態１のプリンタドライバ１１０と同様の機能を有する。ホストＩ／Ｆ制御部１１４は、印刷データとＳＥＥＤをホストＩ／Ｆ１１７からＬＡＮ１５１を介してプリンタ装置１３０に送信するものである。

【００８２】

プリンタ装置５３０には、プリンタコントローラ５４０が装着されており、このプリンタコントローラ５４０は、復号化部５４１と、ＳＥＥＤ元生成部５４２と、ＰＤＬ処理部１４２と、ＰＪＬ処理部１４１と、ホストＩ／Ｆ制御部１４３と、パネル制御部１４４と、蓄積制御部１４５と、印刷制御部１４６とを主に備えている。

【００８３】

ＳＥＥＤ元生成部５４２は、要求を行ったＰＣ５００に対してＳＥＥＤ元を生成して送信するものである。

【００８４】

復号化部５４１は、ＰＣ５００から送信されてきたＳＥＥＤの正当性の判断を行い、正当である場合にＰＣ５００から送信されてきた印刷データをＳＥＥＤによって復号化するものである。

【００８５】

ＰＪＬ処理部１４１は、ＰＣ５００から受信した印刷データに付加されたプリンタジョブ言語（ＰＪＬ：Ｐｒｉｎｔｅｒ　Ｊｏｂ　Ｌａｎｇｕａｇｅ）で記述されたＰＪＬ文書パスワード指定を解釈して、文書パスワードを取得するものである。ＰＪＬ処理部１４１は、この他刷ジョブに関する各種制御を行う。

【００８６】

ＰＤＬ処理部１４２は、ＰＪＬ処理部１４１によって取得された文書パスワードの正当性を判断し、正当である場合には、この文書パスワードを用いて暗号化されたＰＤＦ文書データを復号化し、描画データを生成する。このＰＤＬ処理部１４２は、本発明における文書復号化手段を構成する。

【００８７】

ホストＩ／Ｆ制御部、パネル制御部１４４、蓄積制御部１４５および印刷制御部１４６は、実施の形態１のプリンタコントローラ１４０と同様の機能を有する。

【００８８】

次に、以上のように構成された本実施の形態のプリンタドライバ５１０およびプリンタ装置５３０による暗号化ＰＤＦ文書データの印刷処理について説明する。図６は、本実施の形態のプリンタドライバ５１０およびプリンタ装置５３０による暗号化ＰＤＦ文書データの印刷処理の手順を示すフローチャートである。

【００８９】

まず、ユーザがアプリケーション１２０（Ａｃｒｏｂａｔ（Ｒ）またはＡｃｒｏｂａｔ　Ｒｅａｄｅｒ（Ｒ））でＰＤＦ文書を文書パスワードによって暗号化し、暗号化した状態のままアプリケーション１２０の印刷画面でプリンタ装置１３０のＩＰアドレスを指定して印刷コマンドを発行した場合を考える。

【００９０】

このとき、ジョブ制御部５１３によって、ＰＣ５００のクライアント情報であるＩＰアドレスと、印刷通知と、ＳＥＥＤ元要求とをプリンタ装置５３０に送信する（ステップＳ６０１）。

【００９１】

ＩＰアドレスと、印刷通知と、ＳＥＥＤ元要求とを受信したプリンタ装置５３０では、ＳＥＥＤ元生成部５４２によってＩＰアドレスに固有のＳＥＥＤを生成し、要求元のＰＣ５００に送信する（ステップＳ６０２）。ここで、ＳＥＥＤを生成および送信するタイミングとしては、要求を受けて直ちに行う他、要求を受けてプリンタ装置５３０が印刷可能となった時点で送信するように構成することができる。

【００９２】

ＰＣ５００では、ホストＩ／Ｆ制御部１１４でＳＥＥＤ元を受信すると（ステップＳ６０３）、ＳＥＥＤ生成部５１１によって受信したＳＥＥＤ元からＳＥＥＤを生成する（ステップＳ６０４）。

【００９３】

そして、文書パスワード処理部１１２が文書パスワード入力画面の表示要求をユーザインタフェース部１１３に対して行うことにより、ユーザインタフェース部１１３は文書パスワード入力画面をモニタ１１５に表示する（ステップＳ６０５）。

【００９４】

ユーザが文書パスワード入力画面から暗号化ＰＤＦ文書データに対する文書パスワードをキーボード１１６から入力すると、そのキーイベントをユーザインタフェース部１１３が取得する。そして、文書パスワード処理部１１２は、取得した文書パスワードをＰＪＬ文書パスワード指定データとして暗号化ＰＤＦ文書データの先頭に付加する（ステップＳ６０６）。そして、文書パスワード処理部１１２によって、ＰＪＬ文書パスワード指定データが付加された暗号化ＰＤＦ文書データの後尾にＰＪＬデータを付加し、暗号化部５１２によってこれら３つののデータをＳＥＥＤによって暗号化する（ステップＳ６０７）。

【００９５】

次に、ＰＪＬ文書パスワード指定、暗号化ＰＤＦ文書データおよびＰＪＬデータの３つのデータを暗号化したデータを印刷データとして生成する（ステップＳ６０８）。生成された印刷データは、ＳＥＥＤとともに、ホストＩ／Ｆ制御部１１４によってプリンタ装置１３０に送信される（ステップＳ６０９）。

【００９６】

図７は、本実施の形態のプリンタドライバ５１０で生成される印刷データの構造を示すデータ構造図である。図７に示すように、印刷データは、先頭にＳＥＥＤが付加されており、ＰＪＬ文書パスワード指定（暗号化）と暗号化ＰＤＦ文書データ（暗号化）とＰＪＬデータ（暗号化）とから構成される。なお、ＰＪＬデータは付加されていない場合もある。

【００９７】

プリンタ装置１３０では、ホストＩ／Ｆ制御部１４３で印刷データを受信して（ステップＳ６１０）、復号化部５４１によって受信したＳＥＥＤをＳＥＥＤ元に復号化する（ステップＳ６１１）。復号化部５４１によって、復号化したＳＥ

ＥＤ元と、ＳＥＥＤ元生成部５４２によってステップＳ６０２で生成したＳＥＥＤ元とが一致するか否かを調べることにより、ＳＥＥＤ元の正当性を判断する（ステップＳ６１２）。そして、一致する場合には受信したＳＥＥＤが正当であると判断し、復号化部５４２によってＳＥＥＤ元により印刷データを復号化する（ステップＳ６１３）。一方、両ＳＥＥＤ元が一致しない場合には、受信したＳＥＥＤが不当なものである、すなわちＳＥＥＤが改ざん等されていると判断し、受信した印刷データを破棄し復号化処理を行わない（ステップＳ６１４）。

【００９８】

そして、復号化された印刷データのデータ解釈処理を行い（ステップＳ６１５）、印刷制御部１４６によって印刷実行を行う（ステップＳ６１６）。ここで、データ解釈処理については実施の形態１のプリンタコントローラ１４０と同様の処理で行われる。

【００９９】

なお、本実施の形態では、暗号化ＰＤＦ文書データの印刷時にプリンタドライバ５１０からＳＥＥＤ元の要求をプリンタ装置５３０に行って、ＳＥＥＤ元を取得しているが、この他、プリンタ装置５３０のホストＩ／Ｆ制御部１４３によってネットワーク上でＰＣ５００が接続されたことのブロードキャストメッセージをＰＣ５００から受信して接続を検知した場合に、ＳＥＥＤ元を生成して新たに接続されたＰＣ５００に送信するように構成してもよい。この場合、ＰＣ５００がネットワークに接続された場合、プリンタドライバ５１０のホストＩ／Ｆ制御部１１４によって接続通知のブロードキャストメッセージをプリンタ装置５３０に送信するように構成すれば良い。

【０１００】

このように実施の形態２のプリンタドライバ５１０およびプリンタ装置５３０では、プリンタ装置５３０から取得しＳＥＥＤ元からＳＥＥＤを生成し、アプリケーション１２０によって暗号化されたＰＤＦ文書データを復号化するための文書パスワードと暗号化されたＰＤＦ文書データとを含む印刷データをＳＥＥＤによって暗号化し、暗号化された印刷データとＳＥＥＤをネットワークに接続されたプリンタ装置５３０に送信して、プリンタ装置５３０で復号化して印刷してい

る。すなわち、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書パスワードをＳＥＥＤで暗号化してプリンタ装置に送信するので、ＰＤＦ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置５３０で復号化するまで記憶媒体などにＰＤＦ文書データと文書パスワードを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【０１０１】

なお、本実施の形態では、文書パスワードと暗号化ＰＤＦ文書データの両方をＳＥＥＤで暗号化して印刷データを生成しているが、文書パスワードのみをＳＥＥＤで暗号化して暗号化ＰＤＦ文書データはそのままで印刷データを生成してもよい。これは、ＰＤＦ文書データはすでに文書パスワードによって暗号化されているからである。

【０１０２】

（実施の形態３）

図８は、実施の形態３のクライアント装置（ＰＣ）８００およびプリンタ装置８３０の機能的構成を示すブロック図である。この実施の形態３にかかるＰＣ８００では、ＰＣ上のアプリケーション１２０であるＡｃｒｏｂａｔ（Ｒ）によってＰＤＦ文書データを作成して暗号化し、文書パスワードと文書パスワードの入力で復号化できる暗号化ＰＤＦ文書データを、公開鍵で暗号化して、プリンタ装置８３０に送信し、プリンタ装置８３０で秘密鍵で復号化して印刷するようになっている。

【０１０３】

プリンタ装置８３０とＰＣ８００とは、ＬＡＮ１５１等のネットワークによって接続されている。ＰＣ８００は、図８に示すように、プリンタドライバ８１０がインストールされており、このプリンタドライバ８１０は、ＰＤＬ処理部１１１と、文書パスワード処理部１１２と、暗号化部８１２と、ジョブ制御部８１３と、ユーザインタフェース部１１３と、ホストＩ／Ｆ制御部１１４とを主に備え

ている。

【０１０４】

文書パスワード処理部１１２は、アプリケーション１２０内部で暗号化されたＰＤＦ文書データを復号化するために必要な文書パスワードの入力指示を要求し、入力された文書パスワードを受け付ける。そして、ユーザから入力された文書パスワードをＰＪＬ文書パスワード指定データとして暗号化ＰＤＦ文書データの先頭に付加する。その他の機能は実施の形態１と同様である。

【０１０５】

ジョブ制御部８１３は、プリンタ装置８３０に対して、公開鍵の要求を行うものである。暗号化部８１２は、プリンタ装置８３０から受信した公開鍵によって、ＰＪＬ文書パスワード指定データ、暗号化ＰＤＦ文書データ、および印刷ジョブに関するデータであるＰＪＬデータを暗号化するものである。ＰＤＬ処理部１１１は、実施の形態１のＰＤＬ処理部１１１と同様の機能を有する。

【０１０６】

ユーザインタフェース部１１３は、実施の形態１のプリンタドライバ１１０と同様の機能を有する。ホストＩ／Ｆ制御部１１４は、印刷データとクライアント情報（ＩＰアドレス）をホストＩ／Ｆ１１７からＬＡＮ１５１を介してプリンタ装置１３０に送信するものである。

【０１０７】

プリンタ装置８３０には、プリンタコントローラ８４０が装着されており、このプリンタコントローラ８４０は、復号化部８４１と、秘密鍵生成部と８４２と、公開鍵処理部８４３と、ＰＤＬ処理部１４２と、ＰＪＬ処理部１４１と、ホストＩ／Ｆ制御部１４３と、パネル制御部１４４と、蓄積制御部１４５と、印刷制御部１４６とを主に備えている。

【０１０８】

秘密鍵生成部８４２は、要求を行ったＰＣ８００に対する秘密鍵を生成するものである。公開鍵処理部８４３は、秘密鍵から公開鍵を生成して鍵テーブルに登録し、また生成された公開鍵を要求元のＰＣ８００に送信するものである。

【０１０９】

復号化部８４１は、ＰＣ８００から送信されてきた公開鍵の正当性の判断を行い、正当である場合にＰＣ８００から送信されてきた印刷データを公開鍵に対応する秘密鍵によって復号化するものである。

【０１１０】

ＰＪＬ処理部１４１は、ＰＣ５００から受信した印刷データに付加されたプリンタジョブ言語（ＰＪＬ：Ｐｒｉｎｔｅｒ　Ｊｏｂ　Ｌａｎｇｕａｇｅ）で記述されたＰＪＬ文書パスワード指定を解釈して、文書パスワードを取得するものである。ＰＪＬ処理部１４１は、この他刷ジョブに関する各種制御を行う。

【０１１１】

ＰＤＬ処理部１４２は、ＰＪＬ処理部１４１によって取得された文書パスワードの正当性を判断し、正当である場合には、この文書パスワードを用いて暗号化されたＰＤＦ文書データを復号化し、描画データを生成する。

【０１１２】

ホストＩ／Ｆ制御部、パネル制御部１４４、蓄積制御部１４５および印刷制御部１４６は、実施の形態１のプリンタコントローラ１４０と同様の機能を有する。

【０１１３】

次に、以上のように構成された本実施の形態のプリンタドライバ８１０およびプリンタ装置８３０による暗号化ＰＤＦ文書データの印刷処理について説明する。図９は、本実施の形態のプリンタドライバ８１０およびプリンタ装置８３０による暗号化ＰＤＦ文書データの印刷処理の手順を示すフローチャートである。

【０１１４】

まず、ユーザがアプリケーション１２０（Ａｃｒｏｂａｔ（Ｒ）またはＡｃｒｏｂａｔ　Ｒｅａｄｅｒ（Ｒ））でＰＤＦ文書を文書パスワードによって暗号化し、暗号化した状態のままアプリケーション１２０の印刷画面でプリンタ装置１３０のＩＰアドレスを指定して印刷コマンドを発行した場合を考える。

【０１１５】

このとき、ジョブ制御部８１３によって、ＰＣ８００のクライアント情報であるＩＰアドレスと、印刷通知と、公開鍵要求とをプリンタ装置８３０に送信する

（ステップＳ９０１）。

【０１１６】

ＩＰアドレスと、印刷通知と、公開鍵要求とを受信したプリンタ装置８３０では、秘密鍵生成部８４２によってＩＰアドレスに固有の秘密鍵を生成する（ステップＳ９０２）。そして、公開鍵処理部８４３によって、この秘密鍵から公開鍵を生成し、要求元のＰＣ８００に送信する（ステップＳ９０３）。ここで、公開鍵の生成および送信するタイミングとしては、要求を受けて直ちに行う他、要求を受けてプリンタ装置８３０が印刷可能となった時点で送信するように構成することができる。公開鍵を生成すると、公開鍵処理部８４３によって、鍵テーブルをＨＤＤ１４９に生成し、生成された公開鍵、秘密鍵を登録する（ステップＳ９０４）。

【０１１７】

図１０は、鍵テーブルのデータ構造図である。図１０に示すように、鍵テーブルは、クライアント情報であるＩＰアドレスと公開鍵と秘密鍵と鍵の有効期限とから構成される。

【０１１８】

ＰＣ８００では、ホストＩ／Ｆ制御部１１４で公開鍵を受信すると（ステップＳ９０５）、文書パスワード処理部１１２が文書パスワード入力画面の表示要求をユーザインタフェース部１１３に対して行うことにより、ユーザインタフェース部１１３は文書パスワード入力画面をモニタ１１５に表示する（ステップＳ９０６）。

【０１１９】

ユーザが文書パスワード入力画面から暗号化ＰＤＦ文書データに対する文書パスワードをキーボード１１６から入力すると、そのキーイベントをユーザインタフェース部１１３が取得する。そして、文書パスワード処理部１１２は、取得した文書パスワードをＰＪＬ文書パスワード指定データとして暗号化ＰＤＦ文書データの先頭に付加する（ステップＳ９０７）。そして、ＰＪＬ文書パスワード指定データが付加された暗号化ＰＤＦ文書データの後尾にＰＪＬデータを付加し、暗号化部８１２によってこれら３つのデータを公開鍵によって暗号化する（ステ

ップＳ９０８）。

【０１２０】

次に、ＰＪＬ文書パスワード指定、暗号化ＰＤＦ文書データおよびＰＪＬデータの３つのデータを暗号化したデータを印刷データとして生成する（ステップＳ９０９）。生成された印刷データは、ＰＣ８００のクライアント情報であるＩＰアドレスとともに、ホストＩ／Ｆ制御部１１４によってプリンタ装置８３０に送信される（ステップＳ９１０）。

【０１２１】

図１１は、本実施の形態のプリンタドライバ８１０で生成される印刷データの構造を示すデータ構造図である。図１１に示すように、印刷データは、先頭にクライアント情報（ＩＰアドレス）が付加されており、ＰＪＬ文書パスワード指定（暗号化）と暗号化ＰＤＦ文書データ（暗号化）とＰＪＬデータ（暗号化）とから構成される。なお、ＰＪＬデータは付加されていない場合もある。

【０１２２】

プリンタ装置８３０では、ホストＩ／Ｆ制御部１４３で印刷データを受信して（ステップＳ９１１）、復号化部８４１によって、鍵テーブルを参照し、受信したＩＰアドレスのクライアント情報に対応する公開鍵が有効であるか否かを判断する（ステップＳ９１２）。そして、有効である場合には、復号化部５４２によって秘密鍵で印刷データを復号化する（ステップＳ９１３）。一方、公開鍵が有効でない場合には、受信した印刷データを破棄し復号化処理を行わない（ステップＳ９１６）。

【０１２３】

そして、復号化された印刷データのデータ解釈処理を行い（ステップＳ９１４）、印刷制御部１４６によって印刷実行を行う（ステップＳ９１５）。ここで、データ解釈処理については実施の形態１のプリンタコントローラ１４０と同様の処理で行われる。

【０１２４】

なお、本実施の形態では、暗号化ＰＤＦ文書データの印刷時にプリンタドライバ８１０から公開鍵の要求をプリンタ装置８３０に行って公開鍵を取得している

が、この他、プリンタ装置８３０のホストＩ／Ｆ制御部１４３によってネットワーク上でＰＣ８００が接続されたことのブロードキャストメッセージをＰＣ８００から受信して接続を検知した場合に、秘密鍵、公開鍵を生成して新たに接続されたＰＣ８００に送信するように構成してもよい。この場合、ＰＣ５００がネットワークに接続された場合、プリンタドライバ８１０のホストＩ／Ｆ制御部１１４によって接続通知のブロードキャストメッセージをプリンタ装置８３０に送信するように構成すれば良い。

【０１２５】

このように実施の形態３のプリンタドライバ８１０およびプリンタ装置８３０では、暗号化されたＰＤＦ文書データを復号化せずに、しかも復号化するための文書パスワードを公開鍵で暗号化してプリンタ装置８３０に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができる。また、プリンタ装置８３０で秘密鍵を用いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができる。

【０１２６】

なお、本実施の形態では、文書パスワードと暗号化ＰＤＦ文書データの両方を公開鍵で暗号化して印刷データを生成しているが、文書パスワードのみを公開鍵で暗号化して暗号化ＰＤＦ文書データはそのままで印刷データを生成してもよい。これは、ＰＤＦ文書データはすでに文書パスワードによって暗号化されているからである。

【０１２７】

（実施の形態４）

図１２は、実施の形態４のクライアント装置（ＰＣ）１２００およびプリンタ装置１２３０の機能的構成を示すブロック図である。この実施の形態４にかかるＰＣ１２００では、ＰＣ上のアプリケーション１２０であるＡｃｒｏｂａｔ（Ｒ）によってＰＤＦ文書データを作成して暗号化し、文書パスワードと文書パスワ

ードの入力で復号化できる暗号化ＰＤＦ文書データを公開鍵で暗号化してプリンタ送信すると共に、印刷ジョブに対するジョブパスワードをプリンタ装置８３０に送信し、プリンタ装置１２３０で秘密鍵で復号化して印刷するようになっている。

【０１２８】

プリンタ装置１２３０とＰＣ１２００とは、ＬＡＮ１５１等のネットワークによって接続されている。ＰＣ１２００は、図１２に示すように、プリンタドライバ１２１０がインストールされており、このプリンタドライバ１２１０は、ＰＤＬ処理部１２１２と、文書パスワード処理部１１２と、ジョブパスワード処理部１２１１と、暗号化部８１２と、ジョブ制御部８１３と、ユーザインタフェース部１１３と、ホストＩ／Ｆ制御部１１４とを主に備えている。

【０１２９】

ジョブパスワード処理部１２１１は、印刷ジョブに対するジョブパスワードの入力指示を要求し、入力されたジョブパスワードを受け付ける。そして、ユーザから入力されたジョブパスワードをＰＪＬジョブパスワード指定データとして暗号化ＰＤＦ文書データに付加する。このジョブパスワードは、本発明におけるジョブ認証情報を構成する。ＰＤＬ処理部１２１２は、実施の形態１のＰＤＬ処理部１１１と同様の機能を有する。

【０１３０】

文書パスワード処理部１１２、ユーザインタフェース部１１３、ホストＩ／Ｆ制御部１１４は、実施の形態３のプリンタドライバと同様の機能を有する。

【０１３１】

プリンタ装置１２３０には、プリンタコントローラ１２４０が装着されており、このプリンタコントローラ１２４０は、復号化部１２５４と、秘密鍵生成部８４２と、公開鍵処理部８４３と、ＰＤＬ処理部１４２と、ＰＪＬ処理部１４１と、ホストＩ／Ｆ制御部１４３と、パネル制御部１４４と、蓄積制御部１４５と、印刷制御部１４６とを主に備えている。

【０１３２】

ＰＪＬ処理部１４１は、ＰＣ５００から受信した印刷データに付加されたプリ

ンタジョブ言語（ＰＪＬ：Ｐｒｉｎｔｅｒ　Ｊｏｂ　Ｌａｎｇｕａｇｅ）で記述されたＰＪＬ文書パスワード指定を解釈して文書パスワードを取得するとともに、ＰＪＬジョブパスワード指定を解釈してジョブパスワードを取得するものである。ＰＪＬ処理部１４１は、この他刷ジョブに関する各種制御を行う。

【０１３３】

復号化部８４１、秘密鍵生成部と８４２、公開鍵処理部８４３、ＰＤＬ処理部１４２、ホストＩ／Ｆ制御部１４３、パネル制御部１４４、蓄積制御部１４５は、実施の形態３のプリンタ装置と同様の機能を有している。

【０１３４】

次に、以上のように構成された本実施の形態のプリンタドライバ１２１０およびプリンタ装置１２３０による暗号化ＰＤＦ文書データの印刷処理について説明する。図１３は、本実施の形態のプリンタドライバ１２１０およびプリンタ装置１２３０による暗号化ＰＤＦ文書データの印刷処理の手順を示すフローチャートである。

【０１３５】

まず、ユーザがアプリケーション１２０（Ａｃｒｏｂａｔ（Ｒ）またはＡｃｒｏｂａｔ　Ｒｅａｄｅｒ（Ｒ））でＰＤＦ文書を文書パスワードによって暗号化し、暗号化した状態のままアプリケーション１２０の印刷画面でプリンタ装置１２３０のＩＰアドレスを指定して印刷コマンドを発行した場合を考える。

【０１３６】

このとき、ジョブ制御部８１３によって、ＰＣ１２００のクライアント情報であるＩＰアドレスと、印刷通知と、公開鍵要求とをプリンタ装置１２３０に送信する（ステップＳ１３０１）。

【０１３７】

ＩＰアドレスと、印刷通知と、公開鍵要求とを受信したプリンタ装置１２３０では、秘密鍵生成部８４２によってＩＰアドレスに固有の秘密鍵を生成する（ステップＳ１３０２）。そして、公開鍵処理部８４３によって、この秘密鍵から公開鍵を生成し、要求元のＰＣ８００に送信する（ステップＳ１３０３）。ここで、公開鍵の生成および送信するタイミングとしては、要求を受けて直ちに行う他

、要求を受けてプリンタ装置８３０が印刷可能となった時点で送信するように構成することができる。公開鍵を生成すると、公開鍵処理部８４３によって、鍵テーブルをＨＤＤ１４９に生成し、生成された公開鍵、秘密鍵を登録する（ステップＳ１３０４）。

【０１３８】

ＰＣ１２００では、ホストＩ／Ｆ制御部１１４で公開鍵を受信すると（ステップＳ１３０５）、文書パスワード処理部１１２が文書パスワード入力画面の表示要求を、ジョブパスワード処理部１２１１がジョブパスワード入力画面の表示要求をそれぞれユーザインタフェース部１１３に対して行うことにより、ユーザインタフェース部１１３は文書パスワードおよびジョブパスワード入力画面をモニタ１１５に表示する（ステップＳ１３０６）。

【０１３９】

ユーザが文書パスワード入力画面から暗号化ＰＤＦ文書データに対する文書パスワードを、印刷ジョブに対するジョブパスワードをキーボード１１６からそれぞれ入力すると、そのキーイベントをユーザインタフェース部１１３が取得する。そして、文書パスワード処理部１１２は取得した文書パスワードをＰＪＬ文書パスワード指定データとして暗号化ＰＤＦ文書データに付加し、ジョブパスワード処理部１２１１は取得したジョブパスワードをＰＪＬジョブパスワード指定データとして暗号化ＰＤＦ文書データに付加する（ステップＳ１３０７）。

【０１４０】

そして、ＰＪＬ文書パスワード指定データとＰＪＬジョブパスワード指定データが付加された暗号化ＰＤＦ文書データの後尾にＰＪＬデータを付加し、暗号化部８１２によってこれら３つののデータを公開鍵によって暗号化する（ステップＳ１３０８）。

【０１４１】

次に、ＰＪＬ文書パスワード指定、ＰＪＬジョブパスワード指定、暗号化ＰＤＦ文書データおよびＰＪＬデータの４つのデータを暗号化したデータからページ記述言語を用いて印刷データを生成する（ステップＳ１３０９）。生成された印刷データは、ＰＣ８００のクライアント情報であるＩＰアドレスとともに、ホス

トＩ／Ｆ制御部１１４によってプリンタ装置８３０に送信される（ステップＳ１３１０）。

【０１４２】

図１４は、本実施の形態のプリンタドライバ１２１０で生成される印刷データの構造を示すデータ構造図である。図１４に示すように、印刷データは、先頭にクライアント情報（ＩＰアドレス）が付加されており、ＰＪＬ文書パスワード指定（暗号化）とＰＪＬジョブパスワード指定（暗号化）と暗号化ＰＤＦ文書データ（暗号化）とＰＪＬデータ（暗号化）とから構成される。なお、ＰＪＬデータは付加されていない場合もある。

【０１４３】

プリンタ装置１２３０では、ホストＩ／Ｆ制御部１４３で印刷データを受信して（ステップＳ１３１１）、復号化部８４１によって、鍵テーブルを参照し、受信したＩＰアドレスのクライアント情報に対応する公開鍵が有効であるか否かを判断する（ステップＳ１３１２）。そして、有効である場合には、復号化部５４２によって秘密鍵で印刷データを復号化する（ステップＳ１３１３）。そして、復号化された印刷データのデータ解釈処理を行い（ステップＳ１３１４）、印刷データをＨＤＤ１４９に保存する（ステップＳ１３１５）。ここで、データ解釈処理については実施の形態１のプリンタコントローラ１４０と同様の処理で行われる。一方、公開鍵が有効でない場合には、受信した印刷データを破棄し復号化処理を行わない（ステップＳ１３１８）。

【０１４４】

図１５は、ＨＤＤ１４９に保存される印刷データのデータ構造図である。図１５に示すように、印刷データは、ファイル名と描画データとジョブパスワードとユーザＩＤと日付（ジョブ登録日付）とから構成され、ジョブパスワードとユーザＩＤ、さらにファイル名、日付から検索できるようになっている。

【０１４５】

次に、ＨＤＤ１４９に保存される印刷データを選択するためのジョブ選択処理が行われる（ステップＳ１３１６）。ジョブ選択処理では、まず、パネル制御部１４４が操作パネル１４８にジョブ選択画面を表示する。図１６は、ジョブ選択

画面の流れの一例を示す説明図である。図１６に示すように、ユーザＩＤ、ジョブパスワード、日付、ファイル名を入力することによって、蓄積制御部１４５は入力条件に合致する印刷ジョブの印刷データをＨＤＤ１４９から検索し、パネル制御部１４４によって、その内容を図１６のジョブ一覧画面に表示する。

【０１４６】

ここで、ユーザＩＤ、ジョブパスワードを入力した場合には、そのユーザの全てのジョブがジョブ一覧画面に表示され、さらにファイル名、日付を入力することによって、そのユーザの全てのジョブの中で指定されたファイル名と日付に該当するジョブのみが検索されてジョブ一覧画面に表示されることになる。

【０１４７】

このジョブ一覧からユーザが所望のジョブを選択してＯＫボタンをタッチ操作すると、選択されたジョブに対して、印刷制御部１４６によって印刷実行が行われる（ステップＳ１３１７）。

【０１４８】

なお、本実施の形態のプリンタ装置１２３０では、印刷データのＨＤＤ１４９への保存の処理（ステップＳ１３１３）を、鍵の有効性の判断処理（ステップＳ１３１２）の後に行っているが、ＰＣ１２００から印刷データを受信した時点で、ＨＤＤ１４９に印刷データを保存し、その後、ジョブ選択処理を行って、鍵の有効性の判断処理を行うように構成しても良い。

【０１４９】

また、本実施の形態のプリンタ装置１２３０では、印刷データのＨＤＤ１４９への保存の処理（ステップＳ１３１３）を、データ解釈処理（ステップＳ１３１４）の後、すなわち描画データへの展開後に行っているが、まずジョブの選択処理を行い、その後データ解釈処理を行うように構成しても良い。

【０１５０】

このように実施の形態４のプリンタドライバ８１０およびプリンタ装置８３０では、印刷ジョブを開始させるためのジョブパスワードを含む印刷データを生成して暗号化した上でプリンタ装置１２３０に送信しているので、暗号化されたアプリ文書データの印刷時において、ＰＤＦ文書データを暗号化された状態のまま

、さらに印刷ジョブ毎に認証を行うことができ、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができる。

【０１５１】

なお、本実施の形態のプリンタドライバ１２１０では、ジョブパスワードをユーザに入力させることとしているが、文書パスワードが入力されたときに、ジョブパスワード処理部１２１１によって文書パスワードからジョブパスワードを生成して用いるように構成してもよい。また、この場合、生成するジョブパスワードは、入力された文書パスワードと同一のものとすることも可能である。

【０１５２】

実施の形態１～４では、いずれもＰＤＦ文書データの印刷を例にあげて説明しているが、アプリケーション１２０によって暗号化される文書データであれば、ＰＤＦ文書データに限らず、いずれの文書データにも本発明を適用することが可能である。

【０１５３】

また、実施の形態２～４には、ＰＣのクライアント情報としてＩＰアドレスを使用しているが、例えば、装置固有識別番号等、ＰＣを識別可能なデータであれば、いずれのデータもクライアント情報として使用することができる。

【０１５４】

【発明の効果】

以上説明したように、請求項１にかかる発明によれば、暗号化されたアプリ文書データを復号化せずにプリンタ装置に送信して、同時に送信する文書認証情報によってプリンタ装置側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができ、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

【０１５５】

また、請求項２にかかる発明によれば、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を第２の鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができ、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

【０１５６】

また、請求項３にかかる発明によれば、印刷ジョブごとに異なる第１の鍵情報を取得することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【０１５７】

また、請求項４にかかる発明によれば、印刷する度に第１の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができるという効果を奏する。

【０１５８】

また、請求項５にかかる発明によれば、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を公開鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができ、また、プリンタ装置で秘密鍵情報を用いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

【０１５９】

また、請求項６にかかる発明によれば、印刷ジョブごとに異なる公開鍵情報を取得することができ、暗号化文書の印刷におけるセキュリティをより向上させる

ことができるという効果を奏する。

【０１６０】

また、請求項７にかかる発明によれば、印刷する度に第１の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができるという効果を奏する。

【０１６１】

また、請求項８にかかる発明によれば、暗号化されたアプリ文書データの印刷時において、アプリ文書データを暗号化された状態のまま、さらに印刷ジョブ毎に認証を行うことができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【０１６２】

また、請求項９にかかる発明によれば、印刷ジョブ毎に認証に必要なジョブ認証情報を、アプリ文書データの暗号化に必要な文書認証情報から自動的に生成することができるので、ユーザに何度も認証情報を入力させる手間が省け、ユーザの便宜となるという効果を奏する。

【０１６３】

また、請求項１０にかかる発明によれば、文書認証情報からジョブ認証情報を簡易に生成することができ、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させつつ迅速に行うことができるという効果を奏する。

【０１６４】

また、請求項１１にかかる発明によれば、アプリ文書データを暗号化されたままクライント装置から受信して、同時に送信する文書認証情報によってプリンタ装置側で復号化して印刷を行えるので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを防止することができ、また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データを暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

【０１６５】

また、請求項１２にかかる発明によれば、暗号化されたアプリ文書データを復号化せずに、しかも復号化するための文書認証情報を第２の鍵情報で暗号化してプリンタ装置に送信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができ、また、プリンタ装置で復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

【０１６６】

また、請求項１３にかかる発明によれば、要求された時点で直ちに印刷ジョブごとに異なる第１の鍵情報を送信することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【０１６７】

また、請求項１４にかかる発明によれば、要求があった時点から印刷開始時までに時間差がある場合に、実際に印刷開始時に第１の鍵情報を送信することができるので、要求時点から印刷開始時点までの間に第三者が傍受することを回避することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【０１６８】

また、請求項１５にかかる発明によれば、クライアント装置側で印刷する度に第１の鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができるという効果を奏する。

【０１６９】

また、請求項１６にかかる発明によれば、第１の鍵情報の改ざんされた場合に暗号化されたアプリ文書データの印刷を未然に防止することができ、セキュリティの向上を図ることができるという効果を奏する。

【０１７０】

また、請求項１７にかかる発明によれば、アプリ文書データを暗号化された状態のまま、しかも復号化するための文書認証情報を公開鍵情報で暗号化された状態でクライアント装置から受信するので、アプリ文書データの内容をネットワーク上で悪意のある第三者が傍受することを確実に防止することができ、また、プリンタ装置で秘密鍵情報を用いて復号化するまで記憶媒体などにアプリ文書データと文書認証情報を暗号化された状態で保存することができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティの向上を図ることができるという効果を奏する。

【０１７１】

また、請求項１８にかかる発明によれば、要求された時点で直ちに印刷ジョブごとに異なる公開鍵情報を送信することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【０１７２】

また、請求項１９にかかる発明によれば、要求があった時点から印刷開始時までに時間差がある場合に、実際に印刷開始時に公開鍵情報を送信することができるので、要求時点から印刷開始時点までの間に第三者が傍受することを回避することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【０１７３】

また、請求項２０にかかる発明によれば、クライアント装置側で印刷する度に公開鍵情報を取得する処理が不要となり、暗号化されたアプリ文書データの印刷処理をセキュリティを向上させながら迅速に行うことができるという効果を奏する。

【０１７４】

また、請求項２１にかかる発明によれば、有効期限切れで第三の傍受されたおそれのある秘密鍵情報によるアプリ文書データの復号化および印刷を防止することができ、セキュリティをより向上させることができるという効果を奏する。

【０１７５】

また、請求項２２にかかる発明によれば、暗号化されたアプリ文書データの印刷時において、アプリ文書データを暗号化された状態のまま、さらに印刷ジョブ毎に認証を行うことができるので、悪意のあるシステム管理者によってアプリ文書データの内容を閲覧したり改ざんすることを防止することができ、暗号化文書の印刷におけるセキュリティをより向上させることができるという効果を奏する。

【図面の簡単な説明】

【図１】

実施の形態１のクライアント装置（ＰＣ）およびプリンタ装置の機能的構成を示すブロック図である。

【図２】

実施の形態１のプリンタドライバおよびプリンタ装置による暗号化ＰＤＦ文書データの印刷処理の手順を示すフローチャートである。

【図３】

実施の形態１の印刷データの解釈処理の手順を示すフローチャートである。

【図４】

実施の形態１のプリンタドライバで生成される印刷データの構造を示すデータ構造図である。

【図５】

実施の形態２のクライアント装置（ＰＣ）およびプリンタ装置の機能的構成を示すブロック図である。

【図６】

実施の形態２のプリンタドライバおよびプリンタ装置による暗号化ＰＤＦ文書データの印刷処理の手順を示すフローチャートである。

【図７】

実施の形態２のプリンタドライバで生成される印刷データの構造を示すデータ構造図である。

【図８】

実施の形態３のクライアント装置（ＰＣ）およびプリンタ装置の機能的構成を

示すブロック図である。

【図９】

実施の形態３のプリンタドライバおよびプリンタ装置による暗号化ＰＤＦ文書データの印刷処理の手順を示すフローチャートである。

【図１０】

実施の形態３の鍵テーブルのデータ構造図である。

【図１１】

実施の形態３のプリンタドライバで生成される印刷データの構造を示すデータ構造図である。

【図１２】

実施の形態４のクライアント装置（ＰＣ）およびプリンタ装置の機能的構成を示すブロック図である。

【図１３】

実施の形態４のプリンタドライバおよびプリンタ装置による暗号化ＰＤＦ文書データの印刷処理の手順を示すフローチャートである。

【図１４】

実施の形態４のプリンタドライバで生成される印刷データの構造を示すデータ構造図である。

【図１５】

実施の形態４のプリンタ装置においてＨＤＤに保存される印刷データのデータ構造図である。

【図１６】

実施の形態４のプリンタ装置におけるジョブ選択画面の流れの一例を示す説明図である。

【図１７】

従来のプリンタドライバとプリンタ装置間を流れる印刷データの構造を示すデータ構造図である。

【符号の説明】

１１０，５１０，８１０，１２１０　プリンタドライバ

１１１，１２１２　ＰＤＬ処理部

１１２　文書パスワード処理部

１１３　ユーザインタフェース部

１１５　モニタ

１１６　キーボード

１２０　アプリケーション

１３０，５３０，８３０，１２３０　プリンタ装置

１４０、５４０，８４０，１２４０　プリンタコントローラ

１４１　ＰＪＬ処理部

１４２　ＰＤＬ処理部

１４４　パネル制御部

１４５　蓄積制御部

１４６　印刷制御部

１４８　操作パネル

１４９　ＨＤＤ

１５０　印刷エンジン

５１１　ＳＥＥＤ生成部

５１２　暗号化部

５１３　ジョブ制御部

５４１　復号化部

５４２　ＳＥＥＤ元生成部

８１２　暗号化部

８１３　ジョブ制御部

５４１，８４１，１２５４　復号化部

８４２　秘密鍵生成部

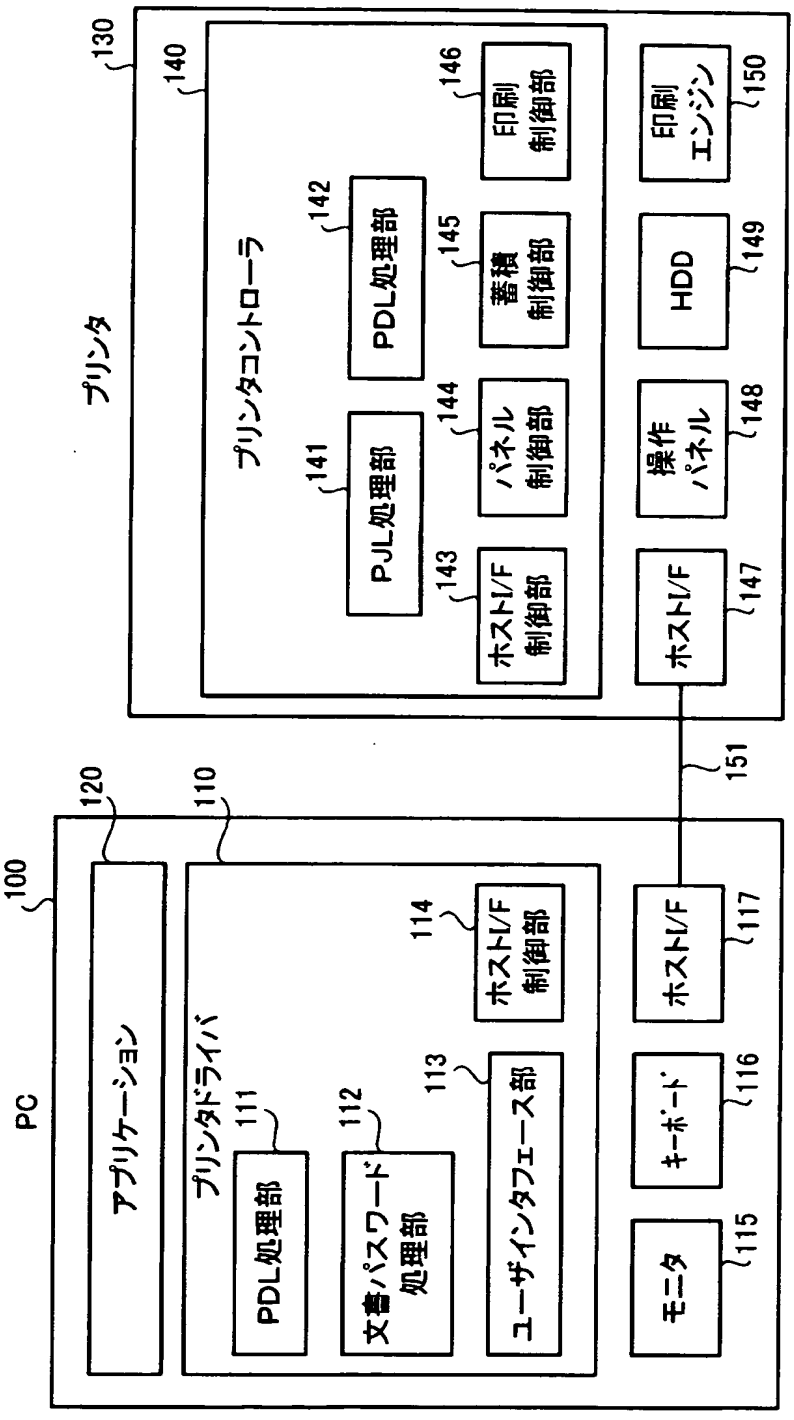
８４３　公開鍵処理部

１２１１　ジョブパスワード処理部

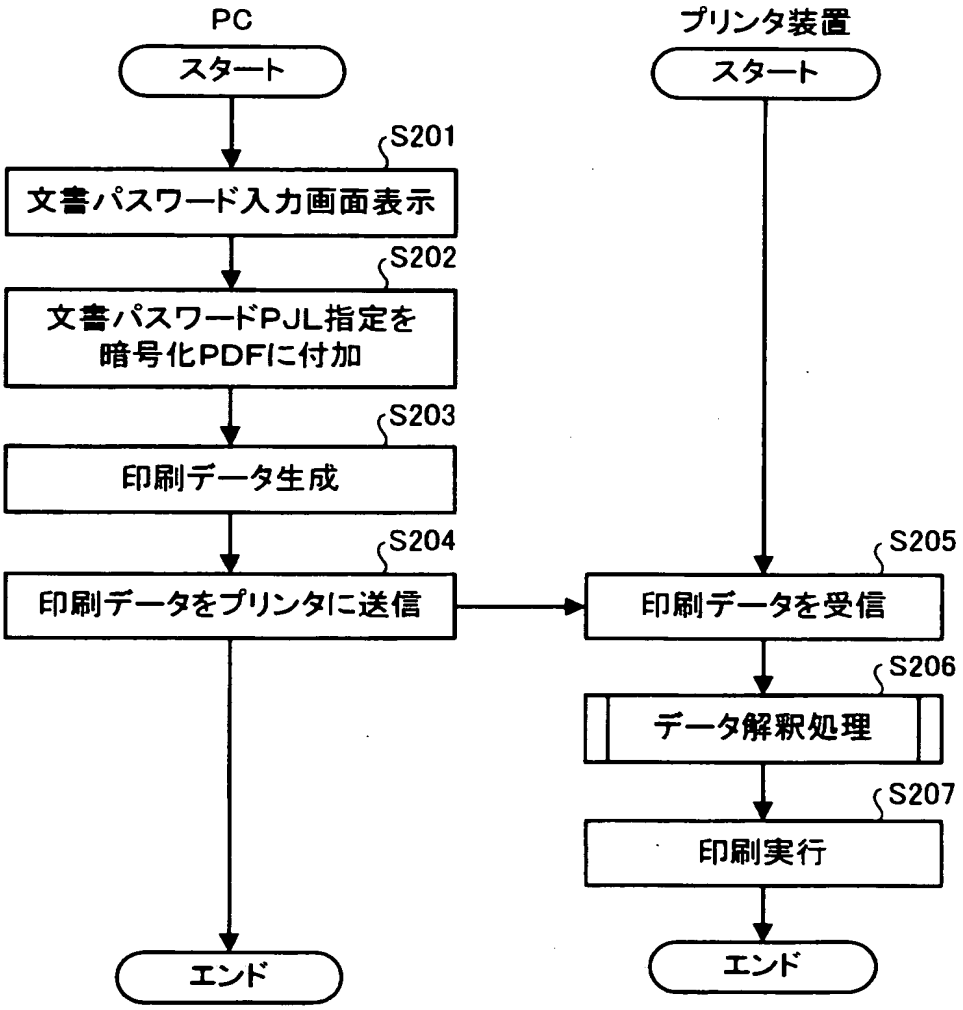
１２４０　プリンタコントローラ

【書類名】　　図面

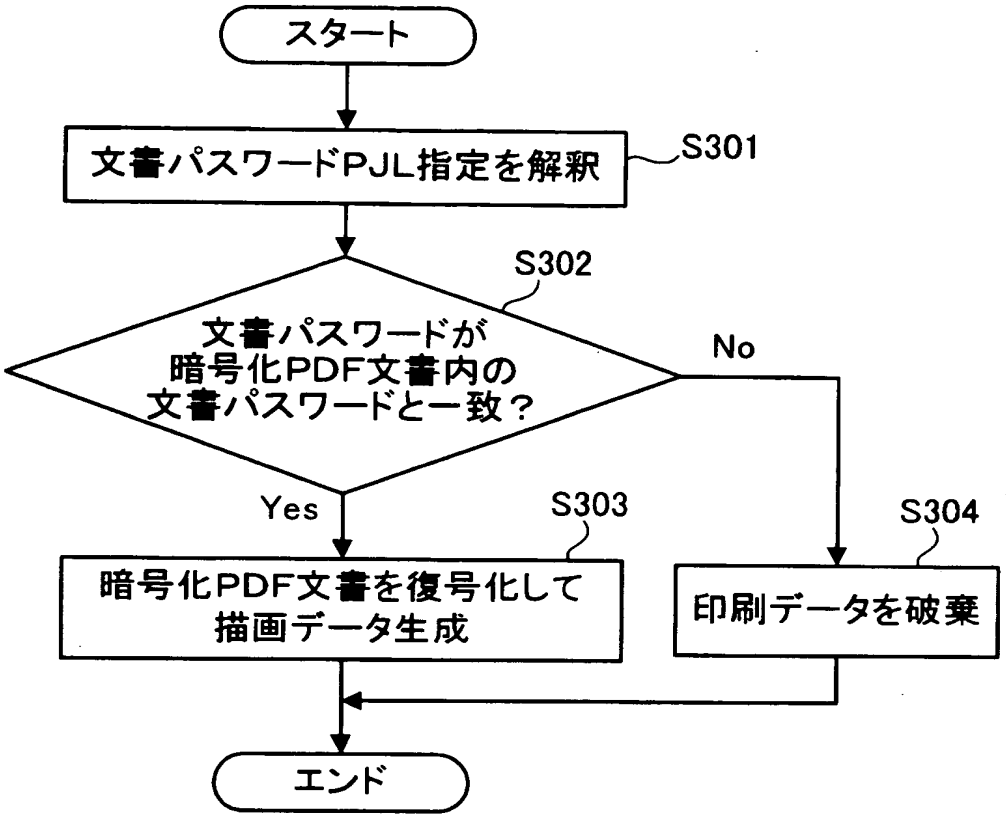
【図１】


PC
100
アプリケーション
120
プリンタドライバ
110
PDL処理部
111
文書パスワード処理部
112
ユーザインタフェース部
113
ホストI/F制御部
114
モニタ
115
キーボード
116
ホストI/F
117
151
プリンタ
130
プリンタコントローラ
140
PJL処理部
141
PDL処理部
142
ホストI/F制御部
143
パネル制御部
144
蓄積制御部
145
印刷制御部
146
ホストI/F
147
操作パネル
148
HDD
149
印刷エンジン
150

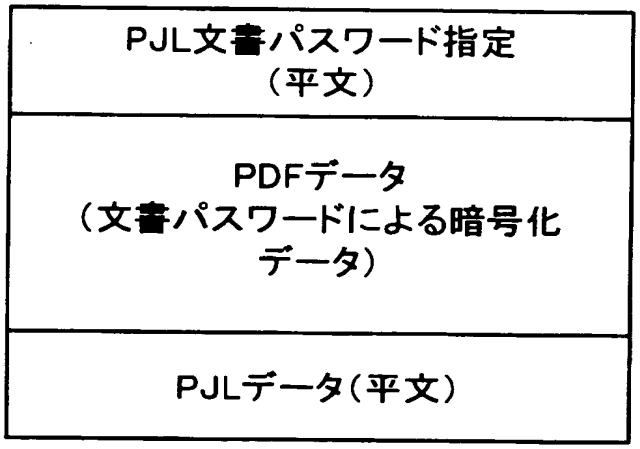
【図２】


PC
スタート
S201
文書パスワード入力画面表示
S202
文書パスワードPJL指定を
暗号化PDFに付加
S203
印刷データ生成
S204
印刷データをプリンタに送信
エンド
プリンタ装置
スタート
S205
印刷データを受信
S206
データ解釈処理
S207
印刷実行
エンド

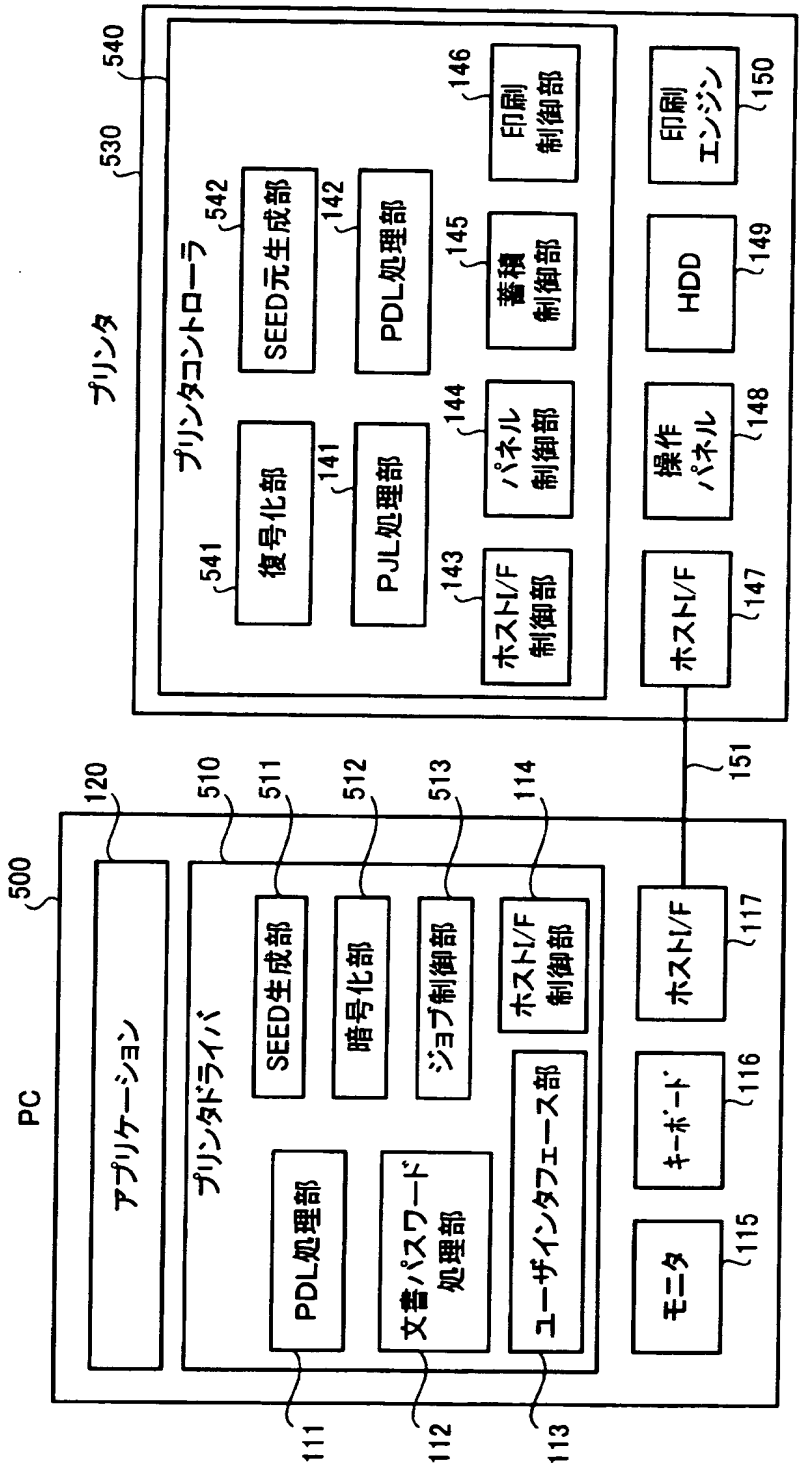
【図３】


スタート
文書パスワードPJL指定を解釈
S301
S302
文書パスワードが
暗号化PDF文書内の
文書パスワードと一致？
No
Yes
S303
S304
暗号化PDF文書を復号化して
描画データ生成
印刷データを破棄
エンド

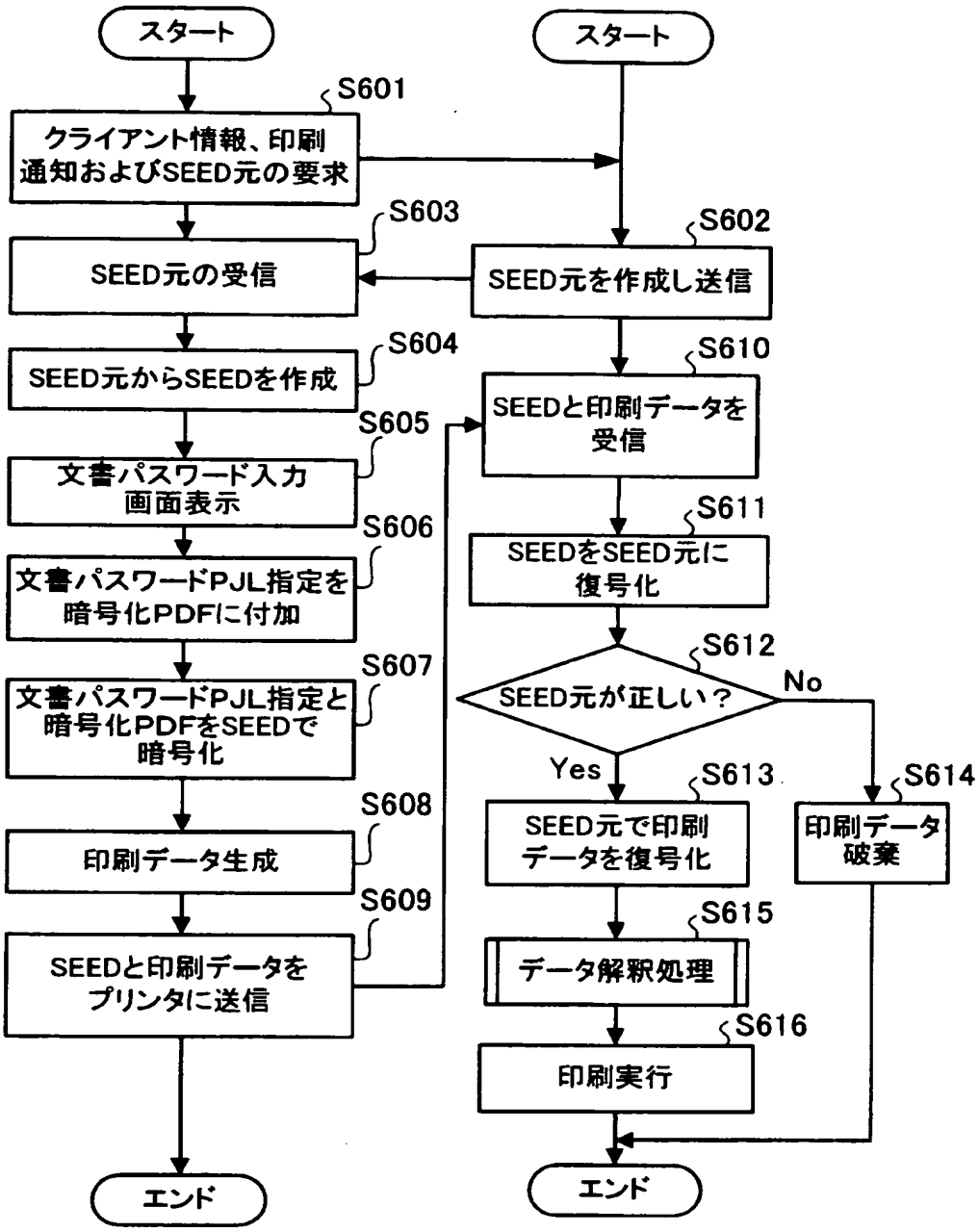
【図４】


PJL文書パスワード指定
（平文）
PDFデータ
（文書パスワードによる暗号化
データ）
PJLデータ（平文）

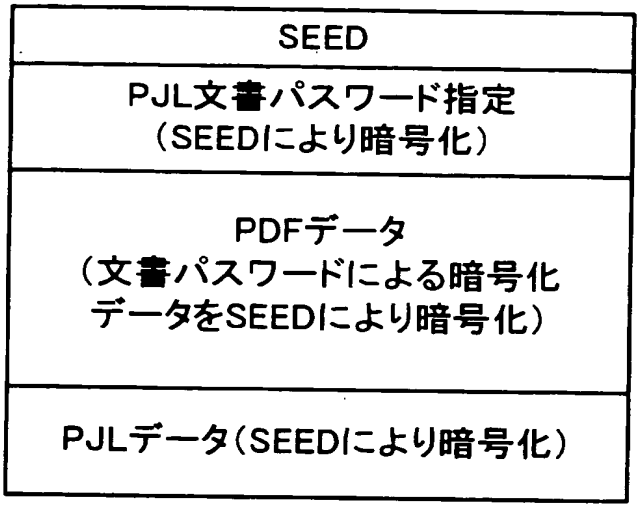
【図５】


PC
500
アプリケーション
120
プリンタドライバ
510
SEED生成部
511
暗号化部
512
ジョブ制御部
513
ホストI/F制御部
114
PDL処理部
111
文書パスワード処理部
112
ユーザインタフェース部
113
モニタ
115
キーボード
116
ホストI/F
117
151
プリンタ
540
プリンタコントローラ
530
SEED元生成部
542
PDL処理部
142
印刷制御部
146
復号化部
541
PJL処理部
141
蓄積制御部
145
パネル制御部
144
ホストI/F制御部
143
HDD
149
印刷エンジン
150
操作パネル
148
ホストI/F
147

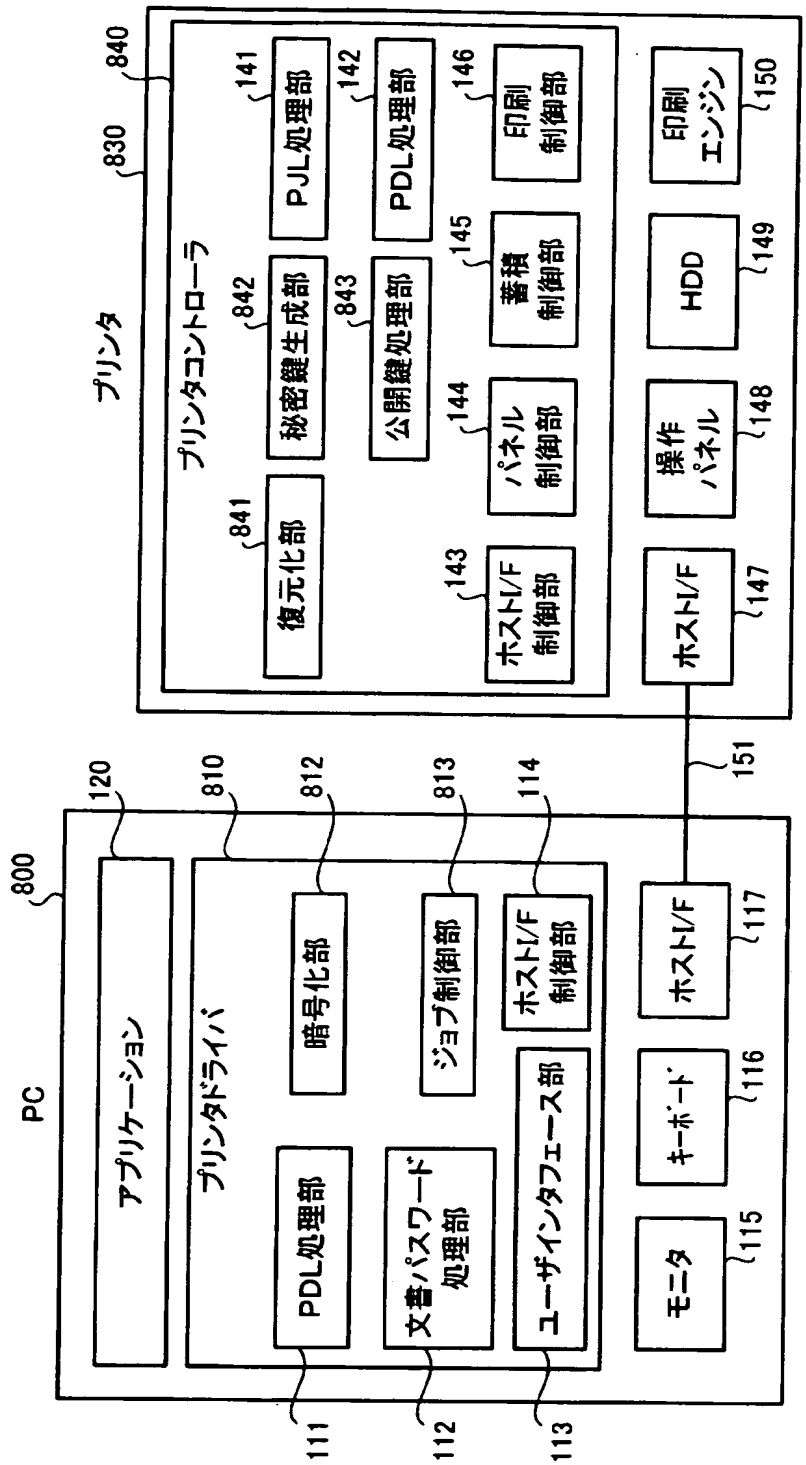
【図６】


スタート
スタート
S601
クライアント情報、印刷通知およびSEED元の要求
S603
SEED元の受信
S602
SEED元を作成し送信
S604
SEED元からSEEDを作成
S610
SEEDと印刷データを受信
S605
文書パスワード入力画面表示
S606
文書パスワードPJL指定を暗号化PDFに付加
S607
文書パスワードPJL指定と暗号化PDFをSEEDで暗号化
S608
印刷データ生成
S609
SEEDと印刷データをプリンタに送信
S611
SEEDをSEED元に復号化
S612
SEED元が正しい？
No
Yes
S613
SEED元で印刷データを復号化
S614
印刷データ破棄
S615
データ解釈処理
S616
印刷実行
エンド
エンド

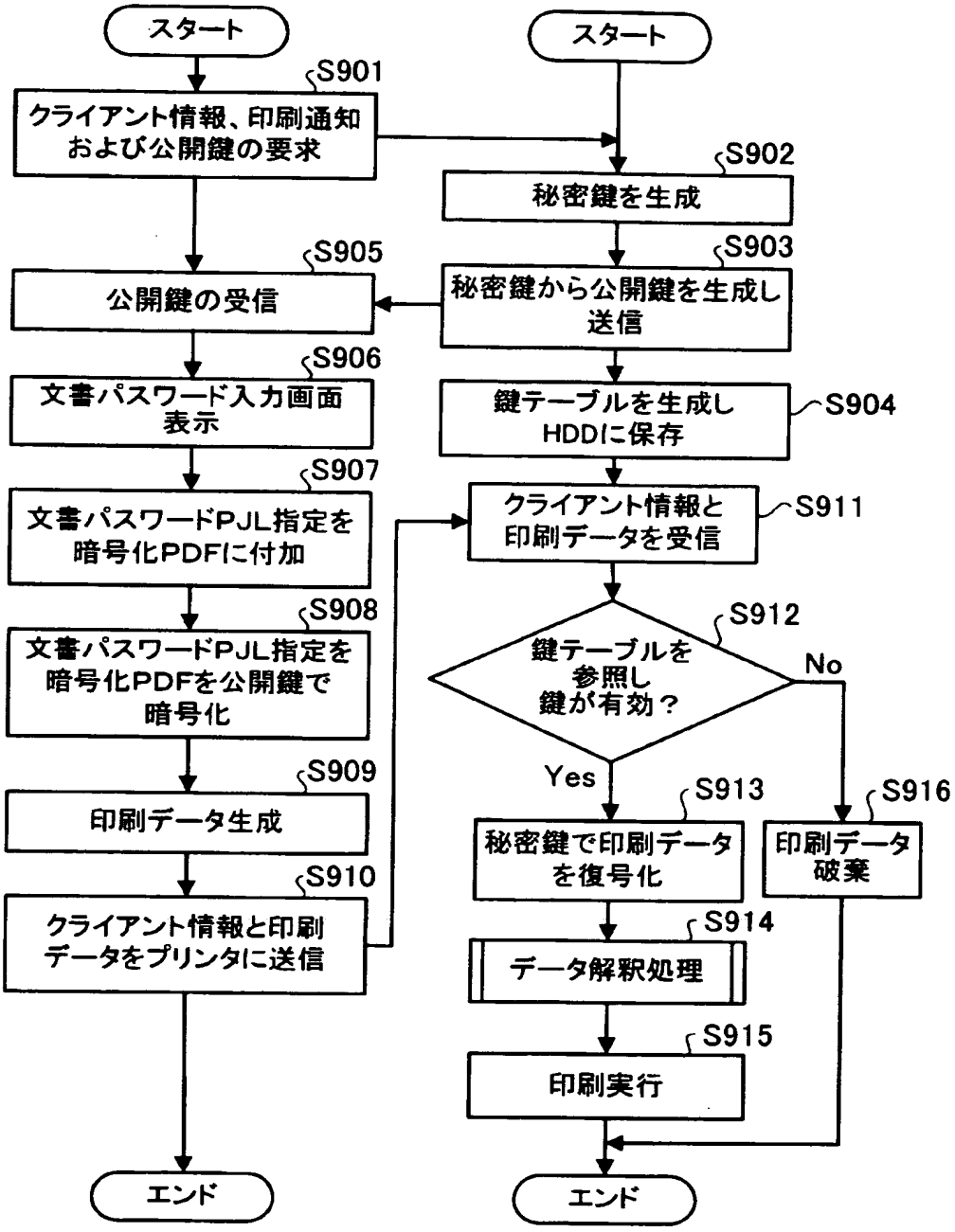
【図７】


SEED
PJL文書パスワード指定
（SEEDにより暗号化）
PDFデータ
（文書パスワードによる暗号化
データをSEEDにより暗号化）
PJLデータ（SEEDにより暗号化）

【図８】


PC
800
アプリケーション
120
プリンタドライバ
810
PDL処理部
111
暗号化部
812
文書パスワード処理部
112
ジョブ制御部
813
ユーザインタフェース部
113
ホストI/F制御部
114
モニタ
115
キーボード
116
ホストI/F
117
151
プリンタ
プリンタコントローラ
830
840
復元化部
841
秘密鍵生成部
842
公開鍵処理部
843
PJL処理部
141
PDL処理部
142
ホストI/F制御部
143
パネル制御部
144
蓄積制御部
145
印刷制御部
146
ホストI/F
147
操作パネル
148
HDD
149
印刷エンジン
150

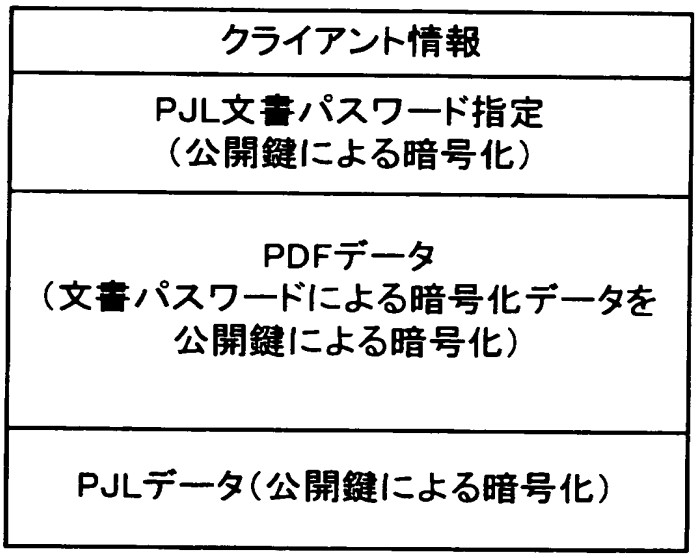
【図９】


スタート
S901
クライアント情報、印刷通知および公開鍵の要求
S905
公開鍵の受信
S906
文書パスワード入力画面表示
S907
文書パスワードPJL指定を暗号化PDFに付加
S908
文書パスワードPJL指定を暗号化PDFを公開鍵で暗号化
S909
印刷データ生成
S910
クライアント情報と印刷データをプリンタに送信
エンド
スタート
S902
秘密鍵を生成
S903
秘密鍵から公開鍵を生成し送信
S904
鍵テーブルを生成しHDDに保存
S911
クライアント情報と印刷データを受信
S912
鍵テーブルを参照し鍵が有効？
No
Yes
S913
秘密鍵で印刷データを復号化
S914
データ解釈処理
S915
印刷実行
S916
印刷データ破棄
エンド

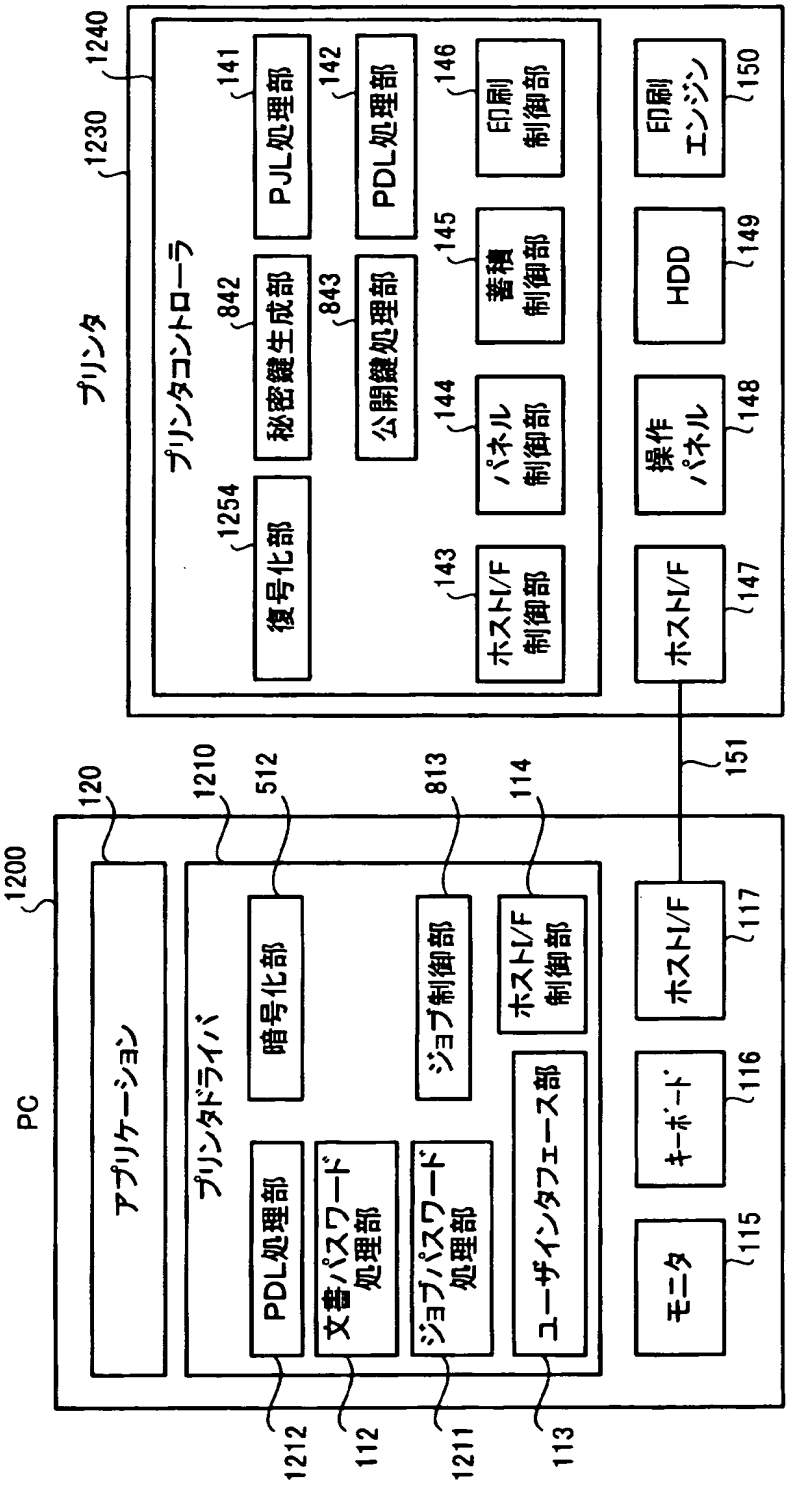
【図１０】

クライアント情報（IPアドレス）	公開鍵	秘密鍵	有効期限

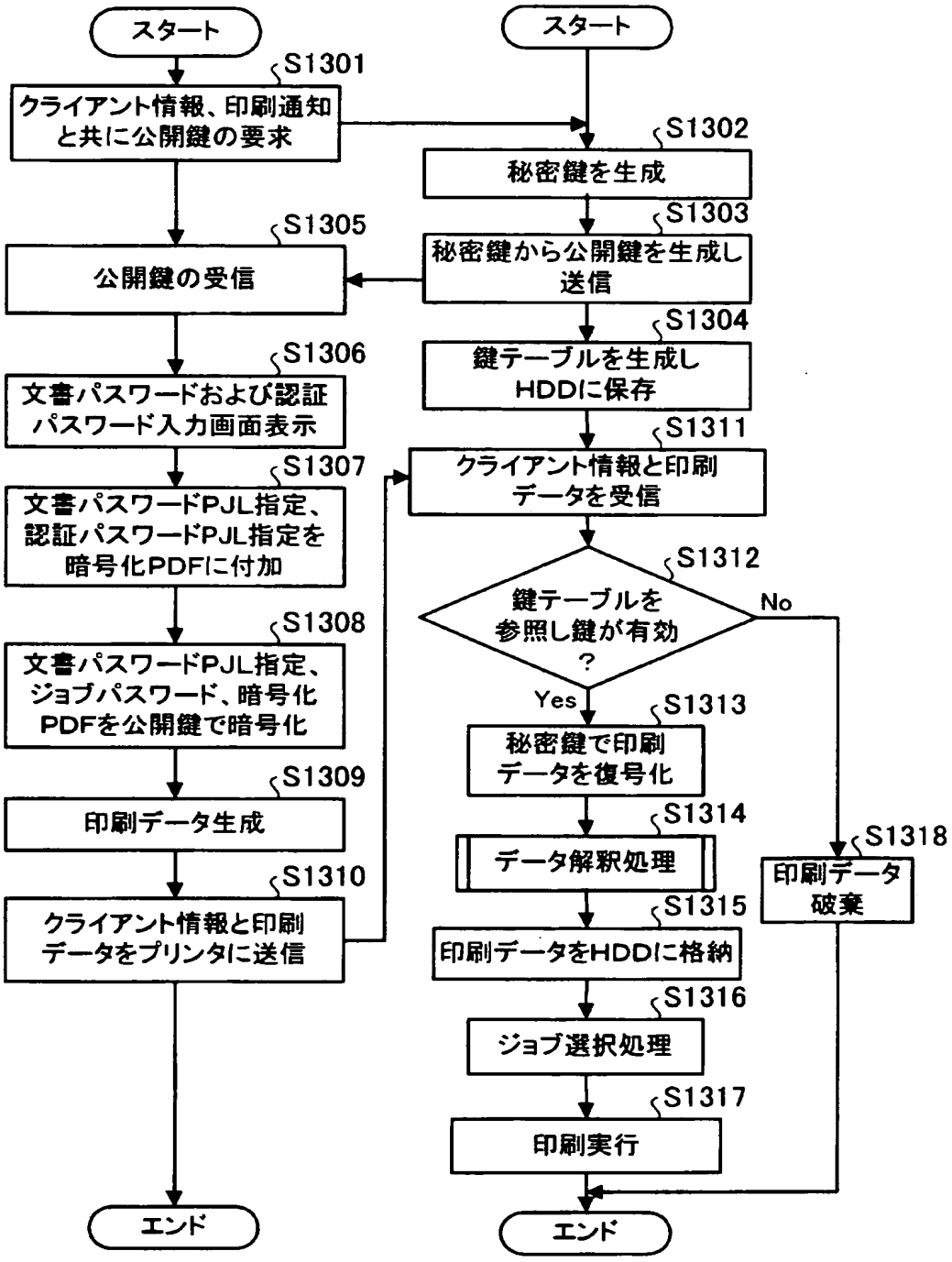
【図１１】



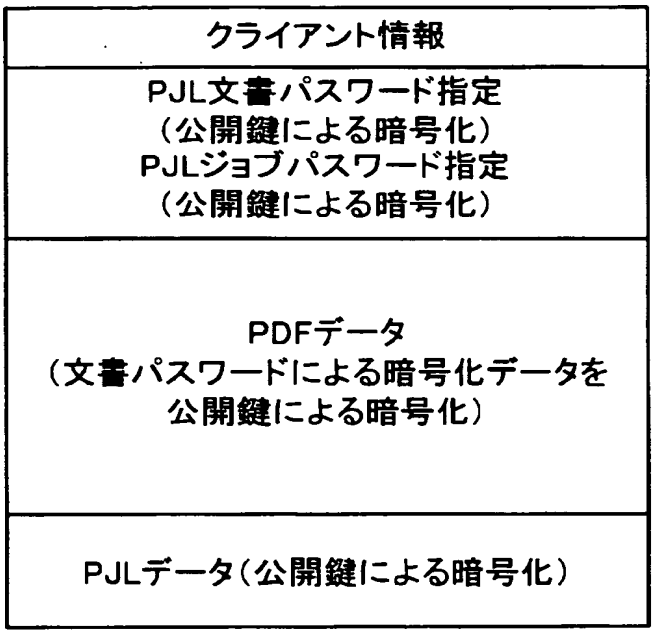
【図１２】


PC
1200
アプリケーション
120
プリンタドライバ
1210
PDL処理部
1212
文書パスワード処理部
112
ジョブパスワード処理部
1211
ユーザインタフェース部
113
暗号化部
512
ジョブ制御部
813
ホストI/F制御部
114
モニタ
115
キーボード
116
ホストI/F
117
151
プリンタ
1240
プリンタコントローラ
1230
復号化部
1254
秘密鍵生成部
842
公開鍵処理部
843
ホストI/F制御部
143
パネル制御部
144
蓄積制御部
145
PJL処理部
141
PDL処理部
142
印刷制御部
146
ホストI/F
147
操作パネル
148
HDD
149
印刷エンジン
150

【図１３】


スタート
S1301
クライアント情報、印刷通知と共に公開鍵の要求
S1305
公開鍵の受信
S1306
文書パスワードおよび認証パスワード入力画面表示
S1307
文書パスワードPJL指定、認証パスワードPJL指定を暗号化PDFに付加
S1308
文書パスワードPJL指定、ジョブパスワード、暗号化PDFを公開鍵で暗号化
S1309
印刷データ生成
S1310
クライアント情報と印刷データをプリンタに送信
エンド
スタート
S1302
秘密鍵を生成
S1303
秘密鍵から公開鍵を生成し送信
S1304
鍵テーブルを生成しHDDに保存
S1311
クライアント情報と印刷データを受信
S1312
鍵テーブルを参照し鍵が有効？
No
Yes
S1313
秘密鍵で印刷データを復号化
S1314
データ解釈処理
S1315
印刷データをHDDに格納
S1316
ジョブ選択処理
S1317
印刷実行
S1318
印刷データ破棄
エンド

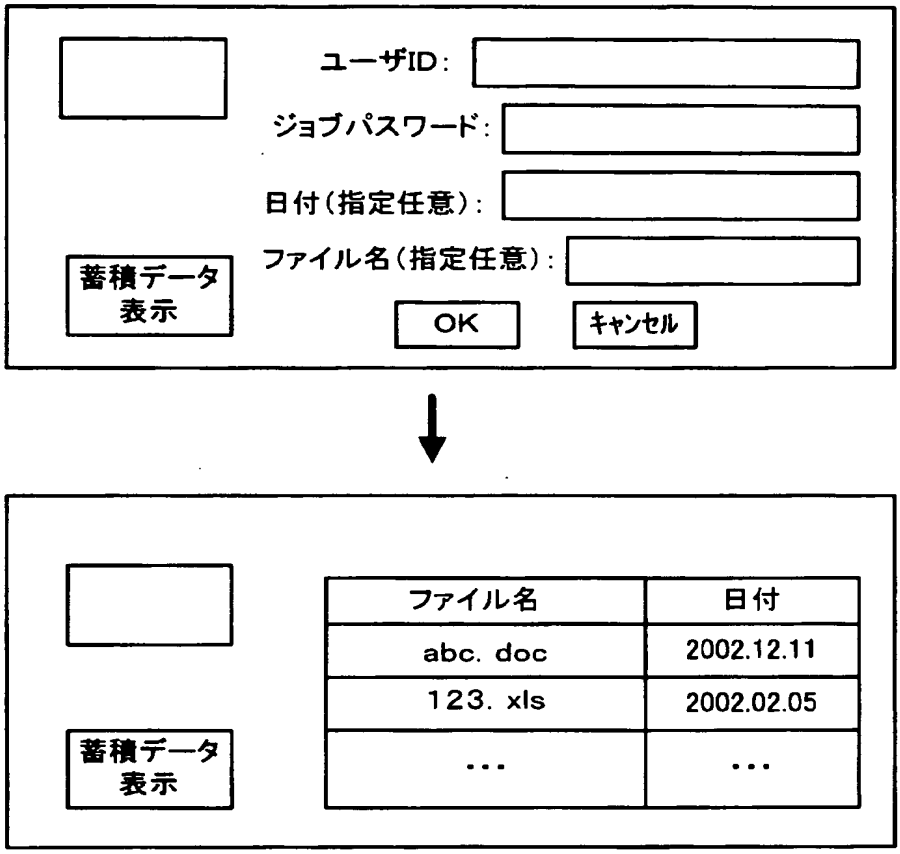
【図１４】


クライアント情報
PJL文書パスワード指定
（公開鍵による暗号化）
PJLジョブパスワード指定
（公開鍵による暗号化）
PDFデータ
（文書パスワードによる暗号化データを
公開鍵による暗号化）
PJLデータ（公開鍵による暗号化）

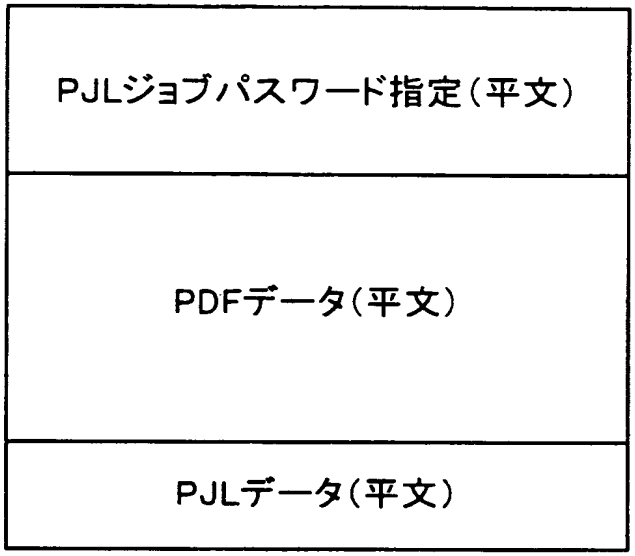
【図１５】


ファイル名
描画データ
ジョブパスワード
ユーザID
日付

【図１６】


ユーザID:
ジョブパスワード:
日付(指定任意):
ファイル名(指定任意):
蓄積データ表示
OK
キャンセル
ファイル名
日付
abc. doc
2002.12.11
123. xls
2002.02.05
...
...
蓄積データ表示

【図１７】



【書類名】　　要約書

【要約】

【課題】　アプリケーションで暗号化された文書データを印刷する場合においてもセキュリティを向上させること。

【解決手段】　ネットワークに接続されたプリンタ装置に対して印刷データを送信して印刷要求を行うプリンタドライバプログラム１１０は、文書パスワード処理部１１２によって、アプリケーション１２０によって暗号化されたＰＤＦ文書データを復号化するための文書パスワードをユーザに入力させる。そして、暗号化されたＰＤＦ文書データと、文書パスワード処理部１１２によって入力された文書パスワードとを含む印刷データを生成する。そして、ホストＩ／Ｆ制御部１１４とホストＩ／Ｆ１１７によって生成された印刷データをネットワーク１５１に接続されたプリンタ装置１３０に送信する。

【選択図】　　図１

特願２００３－０７８７８８

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー